ELSEVIER Linear Algebra and its Applications 345 (2002) 195–224

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

g-Circulant solutions to the (0, 1) matrix equation $A^m = J_n$ ☆

Yao-Kun Wu, Rui-Zhong Jia, Qiao Li*

Department of Applied Mathematics, Shanghai Jiao Tong University, 1954 Huashan Road, Shanghai 200030, China

Received 10 February 2000; accepted 30 August 2001

Submitted by R.A. Brualdi

Abstract

This paper discusses the structure of g-circulant solutions to $A^m = J_n$, where A is an unknown (0, 1) matrix and J_n is a matrix of order n with all entries equal to 1. Wang has made a conjecture on the form of all such solutions. Partially verifying his conjecture, we discover a close relationship among the Hall polynomial $\theta_A(x)$, the shifting parameter g, and the order n of any (0, 1) g-circulant solution A to $A^m = J_n$. As a consequence, all the g-circulant solutions to $A^m = J_n$ are completely determined in the case that n is a prime power. Moreover, in the case that the constant line sum r of A is square-free, all g-circulant solutions to $A^m = J_n$ are proved to be permutation similar to the adjacency matrix of the De Bruijn digraph $B(r, m)$. Motivated by the current status of this subject, we identify all (0, 1) g-circulant solutions to $A^m = J_n$ whose Hall polynomials have some specific properties and we further determine the possible values that the shifting parameter g of such solutions may take. The uniqueness of these solutions up to isomorphism is also investigated. Our paper is concluded with some open problems. In particular, we give the concept of standard factorization and conjecture that all factorizations of $(x^n - 1)/(x - 1)$ into a product of (0, 1) polynomials must be standard and thus point out the close similarity between Wang's conjecture and a conjecture appearing in the study of perfect graph. © 2002 Elsevier Science Inc. All rights reserved.

Keywords: Matrix equation; g-Circulant; Hall polynomial; Shifting parameter; Addition set; Isomorphism; De Bruijn digraph; Standard factorization

☆ Supported by the NNSFC Grant No. 19971056, 10001024 and the RFDP Grant No. 2000024837.

* Corresponding author. Fax: +86-21-628-20892.

E-mail addresses: ykwu@mail1.sjtu.edu.cn (Y.-K. Wu), ruij@hotmail.com (R.-Z. Jia), qiaoli@mail1.sjtu.edu.cn (Q. Li).

PII: S0024-3795(01)00491-8

1. Introduction

Throughout this paper, $\mathbb{N}$ denotes the set of natural numbers and $\mathbb{Z}$ represents the ring of integers whilst $\mathbb{Q}$ and $\mathbb{C}$ denote the field of rational numbers and complex numbers, respectively. We use $\mathbb{Z}^*$ for the set consisting of nonnegative integers, that is, $\mathbb{Z}^* = \mathbb{N} \cup \{0\}$. $\mathbb{Z}^*[x]$ stands for the collection of polynomials with nonnegative integral coefficients. We denote by $\mathbb{Z}_n$ the ring of residues modulo n. For $a, b \in \mathbb{N}$ we define $\mathrm{ord}_a(b)$ to be the maximum integer i such that $a^i \mid b$.

Unless there is additional assumption, all matrices considered in this paper are (0, 1) matrices of size $n \times n$ and we would always let the indices of their rows (columns) run from 0 to $n - 1$. A *permutation matrix* is a (0, 1) matrix with each line (row or column) summing to 1. Two matrices A and B are called *isomorphic* if they are permutation similar, namely, if there exists a permutation matrix P such that $P^{-1}AP = B$. In this case, we shall write $A \cong B$.

The digraph of a matrix A, denoted by $\Gamma(A)$, is defined as the digraph with vertex set $\{0, 1, \dots, n - 1\}$ and there is an edge from vertex i to vertex j if and only if the (i, j) entry of A is 1. It is well known that two (0, 1) matrices A and B are isomorphic if and only if their corresponding digraphs are isomorphic, that is, $A \cong B \iff \Gamma(A) \cong \Gamma(B)$.

Given $s, t \in \mathbb{N}$, the well-known *De Bruijn digraph* $B(s, t)$, which is an important network model studied in computer science, is defined as follows. Its vertex set $V(B(s, t))$ consists of all the t-tuples $(b_1, b_2, \dots, b_t)$ with integral coordinates: $0 \leqslant b_i \leqslant s - 1,\ 1 \leqslant i \leqslant t$; and $(b_1, b_2, \dots, b_t)$ is joined to $(b'_1, b'_2, \dots, b'_t)$ if and only if $b'_i = b_{i+1}$ for $1 \leqslant i \leqslant t - 1$.

For $g \in \mathbb{N}$, a *g-circulant* is a matrix in which each row (except the first) is obtained from the preceding row by shifting the elements cyclically g columns to the right. In other words, the entries of a g-circulant $A = (a_{i,j})$ are related in the manner: $a_{i+1,j} = a_{i,j-g}$, where $0 \leqslant i \leqslant n - 2,\ 0 \leqslant j \leqslant n - 1$, and the subscripts are computed modulo n. Obviously, a g-circulant is uniquely determined by its first row and the *shifting parameter* $g \in \mathbb{N}$. For a g-circulant A, its first row vector, say, $(a_0, a_1, \dots, a_{n-1})$, can be recorded in

$$\theta_A(x) = \sum_{i=0}^{n-1} a_i x^i,$$

which is called the *Hall polynomial* of A. In particular, the Hall polynomial of a (0, 1) g-circulant A can be written as $\theta_A(x) = \sum_{i=0}^{r-1} x^{\alpha_i}$, where $0 \leqslant \alpha_0 < \alpha_1 < \cdots < \alpha_{r-1} \leqslant n - 1$ and $r = \theta_A(1)$. When there is no possibility of ambiguity, we often drop the subscript A and simply write $\theta_A(x)$ as $\theta(x)$. As an example, the reader can check that with the natural vertex order, the adjacency matrix of the De Bruijn digraph $B(s, t)$ is an s-circulant of order s^t with Hall polynomial $1 + x + \cdots + x^{s-1}$.

Let J_n denote the matrix of size $n \times n$ which has all its entries equal to 1. In 1967, Hoffman [11] proposed a famous problem regarding solving the matrix equation $A^2 = J_n$ for an unknown (0, 1) matrix A. Since then it has attracted considerable attention and many authors have contributed to the study of this equation and some other related (0, 1) matrix equations [3,6,7,9,14–35]. However, it turns out that these problems are rather difficult and there are very few general results concerning this particular subject so far. A natural approach, which was adopted by most authors, is to study these (0, 1) matrix equations under special assumptions. Our work in this paper is also some effort in this direction. Loosely speaking, we shall consider g-circulant solutions to the matrix equation

$$A^m = J_n \tag{1}$$

for an unknown (0, 1) matrix A. Although it seems too special to consider only g-circulant solutions, we should mention that this study has some interesting connection with problems arising from perfect graph [1], tiling [4] and large digraph [8].

As any nonnegative integer matrix A satisfying Eq. (1) has to be a (0, 1) matrix, we will sometimes also work with nonnegative integers just for convenience. By a simple result on Hoffman polynomial [12], we know that any nonnegative integer solution A to Eq. (1) must have constant line sum, say r, and $r^m = n$. Since there are only trivial solutions to Eq. (1) when $m = 1$ or $r = n = 1$, we always assume that $m > 1$ and $n > r > 1$. Let $Q_{r,m}$ denote the set of (0, 1) solutions A to Eq. (1) which have constant line sum $r = \theta_A(1)$ and are all g-circulants for some g (here the shifting parameters g are not necessarily the same for different members in the set). One can check that the adjacency matrix of $B(r, m)$ mentioned above is a member of $Q_{r,m}$. In terms of this notation, our purpose can also be interpreted as studying the structure of $Q_{r,m}$.

Let $T_s(x)$ be the polynomial $\sum_{i=0}^{s-1} x^i$ for $s \in \mathbb{N}$ and $T_0(x)$ the constant polynomial 0. A classical result on $Q_{r,m}$ goes as follows:

Theorem 1.1 [17]. *Let A be a g-circulant of order n with $\theta_A(x) = \sum_{i=0}^{r-1} x^{\alpha_i}$. Then $A \in Q_{r,m}$ if and only if $\prod_{i=0}^{m-1} \theta(x^{g^i}) \equiv T_n(x) \pmod{x^n - 1}$.*

The next result is a variation of Theorem 1.1.

Theorem 1.2 [21]. *Let A be a g-circulant and $\theta(x) = \sum_{i=0}^{r-1} x^{\alpha_i}$ its Hall polynomial. Then $A \in Q_{r,m}$ if and only if $\prod_{i=0}^{m-1} \theta(x^{c^i}) \equiv T_n(x) \pmod{x^n - 1}$, where $c = (g, n)$.*

The following theorem is an immediate consequence of Theorems 1.1 and 1.2.

Theorem 1.3. *Suppose that A is a g-circulant and $\theta(x) = \sum_{i=0}^{r-1} x^{\alpha_i}$ is its Hall polynomial. Let $c = (g, n)$. Then the following are equivalent*:

(i) $A^m = J_n$.

(ii) *For each integer i, $0 \leqslant i \leqslant n - 1$, there exists a unique m-tuple $(\alpha_{i_0}, \ldots, \alpha_{i_{m-1}})$, where $\alpha_{i_j} \in \{\alpha_l \colon 0 \leqslant l \leqslant r - 1\}$, $0 \leqslant j \leqslant m - 1$ such that $i \equiv \sum_{j=0}^{m-1} \alpha_{i_j} g^j \pmod{n}$.*

(iii) *For each integer* i, $0 \leqslant i \leqslant n-1$, *there exists a unique m-tuple* $(\alpha_{i_0}, \ldots, \alpha_{i_{m-1}})$, *where* $\alpha_{i_j} \in \{\alpha_l \colon 0 \leqslant l \leqslant r-1\}$, $0 \leqslant j \leqslant m-1$ *such that* $i \equiv \sum_{j=0}^{m-1} \alpha_{i_j} c^j \pmod{n}$.

Theorem 1.3 shows that the study of the g-circulant solutions to Eq. (1) can actually be viewed as a number-theoretical question. Let us describe this question in the language of addition set here. An (n, r, λ, g, m)-*addition set* S is a collection of r residues modulo n such that for any residue $\gamma \not\equiv 0 \pmod{n}$ the congruence

$$\sum_{j=0}^{m-1} s_j g^j \equiv \gamma \pmod{n}$$

has exactly λ solutions $(s_0, s_1, \ldots, s_{m-1})$ with $s_j \in S$, $0 \leqslant j \leqslant m-1$. Note that when $m = 2$ the concept of (n, r, λ, g, m)-addition set defined here coincides with the concept of (n, r, λ, g)-addition set introduced by Lam [18,19]. Let τ be the integer such that $\tau + \lambda$ is the number of ways that 0 can be represented as $\sum_{j=0}^{m-1} s_j g^j \pmod{n}$ with $s_j \in S$, $0 \leqslant j \leqslant m-1$. We call τ the order of the (n, r, λ, g, m)-addition set, generalizing the corresponding concept for difference set in design theory. We shall call an $(n, r, 1, g, m)$-addition set with order 0 a planar (n, r, m)-addition set with shifting parameter g. As with a g-circulant, one can also introduce the Hall polynomial for a subset S of $\mathbb{Z}_n$, which is defined by

$$\theta_S(x) = \sum_{s \in S} x^{s'},$$

where s' is the minimum nonnegative integer in the residue class s. Through this definition we can establish a mapping which sends a g-circulant of order n to a subset of $\mathbb{Z}_n$ with the same Hall polynomial. It is not difficult to see that Theorem 1.3 implies that this mapping actually induces a one to one correspondence between $Q_{r,m}$ and the collection of all the planar (n, r, m)-addition sets. Therefore, finding g-circulant solutions to Eq. (1) is virtually equivalent to constructing planar (n, r, m)-addition sets.

For $c, k, m \in \mathbb{N}$, we write $\Phi_{c,k,m}(x) = \prod_{i=0}^{k-1} T_c(x^{c^{im}})$. The next result is concerning the construction of a class of g-circulant solutions to $A^m = J_n$.

Theorem 1.4 [34]. *Let A be a* $(0, 1)$ *g-circulant satisfying the following conditions*:
(i) $\theta_A(1) = c^k$,
(ii) $g = ct$ *and* $(t, n) = 1$, *and*
(iii) $\Phi_{c,k,m}(x) \mid \theta_A(x)$.
Then $A^m = J_n$.

Let us denote by $P_{c,k,m}$ the set consisting of the g-circulants which satisfy all conditions in Theorem 1.4. Then the foregoing result states that $P_{c,k,m}$ constitutes a subclass of $Q_{c^k,m}$. Conversely, we can show that the members in $Q_{c^k,m}$ bear resemblance to those in $P_{c,k,m}$. To be more precise, for any $(0, 1)$ g-circulant solution

A to Eq. (1), taking $c = (g, n) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, where $p_i,\ 1 \leqslant i \leqslant s$, are distinct primes, our result (see Section 3) asserts:

(i) $\theta(1) = \prod_{i=1}^{s} p_i^{\alpha_i k_i}$ for some $k_i \in \mathbb{N},\ 1 \leqslant i \leqslant s$,

(ii) $(g/c, n) = 1$, and

(iii) $\prod_{i=1}^{s} \Phi_{p_i^{\alpha_i}, k_i, m}(x) \mid \theta(x)$.

The class $P_{c,k,m}$ was first proposed by Wang and Wang in [34], where its members were called the (c, k)-type solutions of Eq. (1). This class has become extremely interesting in the subject we are addressing, as Wang [30,31] has proposed the following conjecture:

Wang's Conjecture. For any (0,1) g-circulant solution A to Eq. (1), there must exist some parameters c and k such that $A \in P_{c,k,m}$.

A consequence of our work mentioned above is that Wang's conjecture is true when n is a prime power and when $\mathrm{ord}_p n = m$ for each prime factor p of n. After knowing our work here, Wang informed us that he has already verified his conjecture in the case that n is a prime power [30]. But the above attracting conjecture still remains far from being settled in general case.

It seems that Wang's conjecture is not an isolated conjecture. We have noticed that in the study of perfect graphs [1,5,10] there also appeared a problem on solving a congruence equation. It was conjectured in [1] that every partitionable graph with circular symmetry is a CGPW graph. At the end of this paper, we will give the concept of standard factorization for a polynomial $(x^n - 1)/(x - 1)$ and then propose the conjecture that all factorizations of $(x^n - 1)/(x - 1)$ into a product of $(0, 1)$ polynomials must be standard factorizations. We will illustrate how does the concept of standard factorization connect all the three conjectures. So, although we are only dealing with g-circulant solutions to Eq. (1) here, we hope that our techniques and results may find usage in a wider range.

Because of Wang's conjecture, it is important to study the construction of the class $P(c, k, m)$ in discussing g-circulant solutions to $A^m = J$. Our paper will provide an enumeration of the set of Hall polynomials of the elements in $P(c, k, m)$ for any given parameters. Thus, from the view-point of generalized addition sets, the structure of $P(c, k, m)$ has been understood quite well. If we view two matrices in a $P(c, k, m)$ being equivalent if and only if their digraphs are isomorphic, the classification of $P(c, k, m)$ will become much more difficult. However, we get some partial results too. More precisely, we will determine for any given parameters c, k, and m whether or not there are two matrices in $P(c, k, m)$ whose digraphs are not isomorphic.

Our paper is organized as follows. In Section 2, we prepare some technical results to be used later. In Section 3, we work out a close relationship among the order n, the Hall polynomial $\theta_A(x)$, and the shifting parameter g for any $(0, 1)$ g-circulant solution A to $A^m = J_n$. In Section 4, we identify the Hall polynomials of the members in $P_{c,k,m}$ and compute the cardinality of $P_{c,k,m}$. This then can be used to give a rather clear picture of the planar (n, r, m)-addition sets in some special cases. In Section 5, for any matrix $A \in Q_{r,m}$, we show that some assumptions on its Hall polynomial, which have close connection with the definition of $P_{c,k,m}$, will considerably restrict the behavior of its shifting parameter. Section 6 is devoted to the study of the uniqueness of the solutions to Eq. (1) up to isomorphism. We show that if a g-circulant (0, 1) matrix A satisfies $A^m = J_n$ and its constant line sum r is squarefree, then $\Gamma(A) \cong B(r, m)$. We also prove that for given $c, k \in \mathbb{N}$ all members in $P_{c,k,m}$ are in the same isomorphism class if and only if $c = k = m = 2$ or one of the three numbers c, k, and m is equal to 1. Finally, we conclude this paper by presenting some open problems in Section 7.

2. Preliminaries

This section includes some lemmas of which we will make use in our work. Most of the polynomials to be dealt with are divisible by $T_c(x^s)$ for some $c, s \in \mathbb{N}$. So we begin by giving some simple properties of such polynomials. For a polynomial $f(x) = \sum_{j=0}^{n-1} a_j x^j$ and $s, i \in \mathbb{Z}$, we write

$$f_{i,s}(x) = \sum_{\substack{j \equiv i \pmod{s} \\ 0 \leqslant j \leqslant n-1}} a_j x^j.$$

Lemma 2.1. *Let* $s, c \in \mathbb{N}$ *and* $f(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{C}[x]$. *If* $T_c(x^s) \mid f(x)$, *then for* $i = 0, 1, \ldots, s-1$, *we have*:

(i) $T_c(x^s) \mid f_{i,s}(x)$.

(ii) $f_{i,s}(x) \equiv (f_{i,s}(1)/c) x^i T_c(x^s) \pmod{x^{cs} - 1}$.

(iii) *If* $f(x) \in \mathbb{Z}^*[x]$, *then* $f_{i,s}(1)/c \in \mathbb{Z}^*$.

(iv) *If* $f(x) \in \mathbb{Z}^*[x]$ *and* $f_{i,s}(1) = c$, *then there exist* $h_0, h_1, \ldots, h_{c-1} \in \mathbb{Z}^*$ *such that* $f_{i,s}(x) = x^i \sum_{j=0}^{c-1} x^{h_j cs + js}$.

(v) *If* $f(x)$ *has nonnegative coefficients and* $f_{i,s}(1) = 0$, *then* $f_{i,s}(x) = 0$.

Proof. (i) Let $f(x) = T_c(x^s)h(x)$. It is easily seen that $f_{i,s}(x) = T_c(x^s)h_{i,s}(x)$.

(ii) For each $0 \leqslant l \leqslant \lfloor (n-1)/s \rfloor$, let $k_l = \lfloor l/c \rfloor$ and $m_l = l - ck_l$. Let

$$q(x) = \sum_{0 \leqslant l \leqslant \lfloor (n-1)/s \rfloor} a_{ls+i} x^{m_l s} = \sum_{j=0}^{c-1} b_j x^{js},$$

where

$$b_j = \sum_{\substack{l \equiv j \pmod{c} \\ 0 \leqslant l \leqslant \lfloor (n-1)/s \rfloor}} a_{ls+i}.$$

Note that it holds $q(1) = f_{i,s}(1) = \sum_{j=0}^{c-1} b_j$.

By the definition of $f_{i,s}(x)$, we have

$$\begin{aligned} f_{i,s}(x) &= x^i \left(\sum_{0 \leqslant l \leqslant \lfloor (n-1)/s \rfloor} a_{ls+i} x^{ls} \right) \\ &= x^i \left(\sum_{0 \leqslant l \leqslant \lfloor (n-1)/s \rfloor} a_{ls+i} x^{k_l cs + m_l s} \right). \end{aligned}$$

By the definition of $q(x)$, we can further write

$$\begin{aligned} f_{i,s}(x) &= x^i q(x) + x^i \left(\sum_{0 \leqslant l \leqslant \lfloor (n-1)/s \rfloor} a_{ls+i} (x^{k_l cs} - 1) x^{m_l s} \right) \\ &\equiv x^i q(x) \pmod{x^{cs} - 1}. \end{aligned} \tag{2}$$

The last equality is due to the fact that $x^{cs} - 1 \mid x^{k_l cs} - 1$ for all l.

Now (i) together with the fact that $T_c(x^s) \mid x^{cs} - 1$ implies $T_c(x^s) \mid x^i q(x)$. Since $(T_c(x^s), x^i) = 1$, we see that $T_c(x^s) \mid q(x)$. But the degree of $q(x)$ is at most $s(c-1)$, while $T_c(x^s)$ is a polynomial whose degree is exactly $s(c-1)$. This shows that

$$q(x) = aT_c(x^s) \tag{3}$$

for some constant number a. Putting $x = 1$ in (3) yields $a = q(1)/c = f_{i,s}(1)/c$. So (3) can be rewritten as

$$q(x) = \big(f_{i,s}(1)/c\big) T_c(x^s). \tag{4}$$

Now (2) implies that $f_{i,s}(x) \equiv (f_{i,s}(1)/c) x^i T_c(x^s) \pmod{x^{cs} - 1}$, as required.

(iii) From $f(x) \in \mathbb{Z}^*[x]$, it easily follows $q(x) \in \mathbb{Z}^*[x]$ and thus (4) implies $f_{i,s}(1)/c \in \mathbb{Z}^*$.

(iv) Since $f_{i,s}(1) = c$, (4) says $q(x) = T_c(x^s)$. So

$$b_j = \sum_{\substack{l \equiv j \pmod{c} \\ 0 \leqslant l \leqslant \lfloor (n-1)/s \rfloor}} a_{ls+i} = 1$$

for $j = 0, 1, \ldots, c-1$. Since it is assumed that $f(x) \in \mathbb{Z}^*[x]$, we immediately find that for each $j = 0, 1, \ldots, c-1$, all a_{ls+i}, where $l \equiv j \pmod{c}$ and $0 \leqslant l \leqslant \lfloor (n-1)/s \rfloor$, are equal to zero with exactly one exception and the exceptional value is 1. This illustrates that there exists $h_j \in \mathbb{Z}^*$ for each $j \in \{0, 1, \ldots, c-1\}$ such that $f_{i,s}(x) = x^i \sum_{j=0}^{c-1} x^{h_j cs + js}$, which is the result.

(v) The assumption means that the coefficients of $f_{i,s}(x)$ are all nonnegative and sum to 0. Hence they all must be 0. □

Corollary 2.1. *If $f(x) \in \mathbb{Z}^*[x]$, $f(1) = n$, and $T_n(x) \mid f(x)$, then there exist h_0, $h_1, \ldots, h_{n-1} \in \mathbb{Z}^*$ such that $f(x) = \sum_{j=0}^{n-1} x^{h_j n+j}$.*

Proof. Note that $f(x) = f_{0,1}(x)$ and then apply Lemma 2.1(iv). □

For a polynomial $f(x)$, let Root$(f(x))$ denote the collection of all distinct roots of $f(x) = 0$ in the field $\mathbb{C}$. For a root of unity, say ξ, the minimum positive integer t such that $\xi^t = 1$ is called the order of ξ. We use $\phi_n(x)$ to denote the nth cyclotomic polynomial.

The following lemma describes a basic property of $T_r(x^s)$ which will be frequently cited afterwards.

Lemma 2.2. *Let $f(x) \in \mathbb{Z}^*[x]$ and $c, k, m \in \mathbb{N}$. If $\Phi_{c,k,m}(x) | f(x)$ in $\mathbb{C}[x]$, then $f(1) \geqslant c^k$. If $f(1) = c^k$, then $f(x)$ must be a* (0, 1) *polynomial, namely, a polynomial each of whose coefficients is either* 0 *or* 1, *and $h(x) \equiv T_n(x)$* (mod $x^n - 1$), *where $n = c^{km}$ and $h(x) = \prod_{i=0}^{m-1} f\left(x^{c^i}\right)$.*

Proof. Recall that $\Phi_{c,k,m}(x) = \prod_{i=0}^{k-1} T_c\left(x^{c^{im}}\right)$. It is easily seen that $\prod_{i=0}^{m-1} \Phi_{c,k,m}(x^{c^i}) = T_n(x)$. Hence by hypothesis, there is $g(x)$ such that $h(x) = T_n(x)g(x)$. Since $T_n(x), h(x) \in \mathbb{Z}[x]$ and $T_n(x)$ is monic, we then get $g(x) \in \mathbb{Z}[x]$. By setting $x = 1$, we immediately obtain $f(1)^m = h(1) \geqslant T_n(1) = c^{km}$ and hence $f(1) \geqslant c^k$. If $f(1) = k$, then $h(1) = n$. Thus we can deduce from Corollary 2.1 that $h(x)$ is a (0, 1) polynomial and $h(x) \equiv T_n(x)$ (mod $x^n - 1$). Because $h(x) = \prod_{i=0}^{m-1} f(x^{c^i})$ and $f(x) \in \mathbb{Z}^*[x]$, we see that $f(x)$ is a (0, 1) polynomial too. □

Lemma 2.3. *Let $f(x) \in \mathbb{Z}^*[x]$ and $c, k, m \in \mathbb{N}$. If $\Phi_{c,k,m}(x) | f(x)$ in $\mathbb{C}[x]$, then $f(1) \geqslant c^k$. If $f(1) = c^k$, then $f(x)$ must be a* (0, 1) *polynomial, namely, a polynomial each of whose coefficients is either* 0 *or* 1, *and $\prod_{i=0}^{m-1} f(x^{c^i}) \equiv T_n(x)$* (mod $x^n - 1$).

Proof. Recall that $\Phi_{c,k,m}(x) = \prod_{i=0}^{k-1} T_c(x^{c^{im}})$. Write $n = c^{km}$ and $h(x) = \prod_{i=0}^{m-1} f(x^{c^i})$. It is easily seen that $\prod_{i=0}^{m-1} \Phi_{c,k,m}(x^{c^i}) = T_n(x)$. Hence by hypothesis, there is $g(x)$ such that $h(x) = T_n(x)g(x)$. Since $T_n(x), h(x) \in \mathbb{Z}[x]$ and $T_n(x)$ is monic, we then get $g(x) \in \mathbb{Z}[x]$. By setting $x = 1$, we immediately obtain $f(1)^m = h(1) \geqslant T_n(1) = c^{km}$ and hence $f(1) \geqslant c^k$. If the equality holds, $h(1) = n$. We then obtain from Corollary 2.1 that $h(x)$ is a $(0, 1)$ polynomial and $h(x) \equiv T_n(x)$ (mod $x^n - 1$). Because $h(x) = \prod_{i=0}^{m-1} f(x^{c^i})$ and $f(x) \in \mathbb{Z}^*[x]$, we see that $f(x)$ is a (0, 1) polynomial too. □

Let $F_n = \{\sum_{0 \leqslant i \leqslant n-1} x^{a_i n+i} : a_i \in \mathbb{Z}^*\}$. The reason for our interest in F_n is clarified in the next result.

Lemma 2.4. *If* $h(x) \in \mathbb{Z}^*[x]$ *and* $h(x) \equiv T_n(x) \pmod{x^n - 1}$, *then* $h(x) \in F_n$.

Proof. We deduce from $h(x) \equiv T_n(x) \pmod{x^n - 1}$ that $T_n(x) \mid h(x)$ and $h(1) = n$. Thus our statement here is actually the same as that in Corollary 2.1. □

In the sequel, we recall a result (see [13, p. 301, Example 5(f)]), which can be easily deduced from the fact $x^l - 1 = \prod_{d \mid l} \phi_d(x)$ for all $l \in \mathbb{N}$.

Lemma 2.5.

$$\phi_n(1) = \begin{cases} 0 & \text{if } n = 1, \\ p & \text{if } n = p^k, \text{ where } p \text{ is a prime and } k > 0, \\ 1 & \text{otherwise.} \end{cases}$$

Our next lemma is a basic observation on the members of F_n and can be established by a direct calculation.

Lemma 2.6. *Let* $a_i \in \mathbb{Z}^*$ *for* $i = 0, 1, \ldots, n - 1$. *Then*

$$\sum_{i=0}^{n-1} x^{a_i n + i} = T_n(x) \left(1 + (x - 1)\left(\sum_{i=0}^{n-1} x^i T_{a_i}(x^n)\right)\right).$$

The “if” part of the forthcoming lemma plays a crucial role in our work in Section 3 while its “only if” part, which is not used in the current paper, will explain why our efforts here did not result in a complete resolution to the problem we are discussing.

Lemma 2.7. *Let* $\xi \neq 1$ *be an* nth *root of unity and* t *the order of* ξ. *Then* ξ *is a simple root of* $f(x) = 0$ *for all* $f(x) \in F_n$ *if and only if* t *is a prime power.*

Proof. It is certainly true that ξ is a simple root of $T_n(x) = 0$. Hence Lemma 2.6 implies that our assertion is equivalent to the following: none of the polynomials $1 + (x - 1)(\sum_{i=0}^{n-1} x^i T_{a_i}(x^n))$, where $a_i \in \mathbb{Z}^*$, will vanish at $x = \xi$ if and only if t is a prime power.

First suppose that there exist $a_0, \ldots, a_{n-1} \in \mathbb{Z}^*$ such that $1 + (\xi - 1)(\sum_{i=0}^{n-1} \xi^i T_{a_i}(\xi^n)) = 0$. Then $1 + (\xi - 1)(\sum_{i=0}^{n-1} a_i \xi^i) = 0$ as $\xi^n = 1$. Note that the minimal polynomial of ξ over Q is $\phi_t(x)$. Hence, if we denote the polynomial $1 + (x - 1)(\sum_{i=0}^{n-1} a_i x^i)$ by $g(x)$, then $g(x)$ is a multiple of $\phi_t(x)$ in the polynomial ring $\mathbb{Z}[x]$. In particular, it follows that $g(1)$ (which is equal to 1) is a multiple of $\phi_t(1)$ in $\mathbb{Z}$, which implies then $\phi_t(1)$ has absolute value 1. By Lemma 2.5, t has at least two distinct prime factors.

Conversely, assume that $t \neq 1$ is not a prime power. Then, again by Lemma 2.5, $\phi_t(1) = 1$. This ensures that $\phi_t(x) - 1 = (x - 1)u(x)$ for some $u(x) \in \mathbb{Z}[x]$.

Comparing the degrees of the polynomials on both sides, we find that deg $u(x) <$ deg $\phi_t(x) < n$. This enables us to write $u(x) = \sum_{i=0}^{n-1} d_i x^i$ with $d_i \in \mathbb{Z}$ for $0 \leqslant i \leqslant n-1$. Let $\delta = \min\{d_i : 0 \leqslant i \leqslant n-1\}$ and define $a_i = d_i - \delta$ for each i. Then $a_i \in \mathbb{Z}^*$, $0 \leqslant i \leqslant n-1$. Consequently,

$$\begin{aligned}1 + (\xi - 1)\left(\sum_{i=0}^{n-1} \xi^i T_{a_i}(\xi^n)\right) &= 1 + (\xi - 1)\left(\delta T_n(\xi) + \sum_{i=0}^{n-1} a_i \xi^i\right)\\ &= 1 + (\xi - 1)u(\xi)\\ &= \phi_t(\xi)\\ &= 0.\end{aligned}$$

This asserts that the polynomial $1 + (x-1)(\sum_{i=0}^{n-1} x^i T_{a_i}(x^n))$ vanishes at $x = \xi$ and thus the proof is ended. □

Let us conclude this section by presenting two more lemmas.

Lemma 2.8. *Let d, n, g be positive integers with $d \mid (g, n)$. Suppose that $\theta(x) \in \mathbb{C}[x]$ and $\theta(1) \neq 0$. If $\prod_{i=0}^{m-1} \theta(x^{g^i}) \equiv T_n(x) \pmod{x^n - 1}$, then $T_d(x) \mid \theta(x)$ in $\mathbb{C}[x]$. Furthermore, $T_d(x) \mid \theta(x)$ in $\mathbb{Z}[x]$ whenever $\theta(x) \in \mathbb{Z}[x]$.*

Proof. By setting x to be each of the nontrivial dth roots of unity in $\prod_{i=0}^{m-1} \theta(x^{g^i}) \equiv T_n(x) \pmod{x^n - 1}$, we obtain $\mathrm{Root}(T_d(x)) \subseteq \mathrm{Root}(\theta(x))$. Since $T_d(x)$ has no multiple roots, we conclude that $T_d(x) \mid \theta(x)$ in $\mathbb{C}[x]$. Further, as $T_d(x) \in \mathbb{Z}[x]$ is a monic polynomial, we can get from $\theta(x) \in \mathbb{Z}[x]$ that $\theta(x)/T_d(x) \in \mathbb{Z}[x]$, which completes the proof. □

Lemma 2.9. *Let c, b be two natural numbers such that $\mathrm{ord}_b(c) = \alpha$ and $(d, b) = 1$, where $d = c/b^\alpha$. Suppose that $\theta(x) \in \mathbb{Z}[x]$. Then the following hold for $i, j, k \in \mathbb{Z}^*$:*

(i) *If $\mathrm{Root}(T_{b^k}(x^{b^j})) \subseteq \mathrm{Root}(\theta(x))$, then $T_{b^k}(x^{b^{j+i\alpha}}) \mid \theta(x^{c^i})$ in $\mathbb{Z}[x]$.*

(ii) *Let $i \geqslant 1$, $j \geqslant \alpha$. Then $\mathrm{Root}(T_{b^k}(x^{b^j})) \cap \mathrm{Root}(\theta(x^{c^i})) \neq \emptyset$ implies $\mathrm{Root}(T_{b^k}(x^{b^{j-\alpha}})) \cap \mathrm{Root}(\theta(x^{c^{i-1}})) \neq \emptyset$.*

Proof. (i) Let ξ be a root of $T_{b^k}(x^{b^{j+i\alpha}}) = 0$. Then, by Lemma 2.2, ξ is a tth primitive root of unity for some t with $t \nmid b^{j+i\alpha}$ and $t | b^{j+i\alpha+k}$. Hence, the order of $\xi^{b^{i\alpha}}$, say t', should satisfy $t' \nmid b^j$ but $t' | b^{j+k}$. Now $(d, b) = 1$ together with $t' | b^{j+k}$ implies that $\xi^{c^i} = \xi^{b^{i\alpha} d^i}$ also has order t'. From Lemma 2.2 and the assumption $\mathrm{Root}(T_{b^k}(x^{b^j})) \subseteq \mathrm{Root}(\theta(x))$, we can deduce that $\xi^{c^i} \in \mathrm{Root}(\theta(x))$. Consequently, $\xi \in \mathrm{Root}(\theta(x^{c^i}))$. So we have arrived at $\mathrm{Root}(T_{b^k}(x^{b^{j+i\alpha}})) \subseteq \mathrm{Root}(\theta(x^{c^i}))$. Because $T_{b^k}(x^{b^{j+i\alpha}})$ has no multiple roots (see Lemma 2.2), we get $T_{b^k}(x^{b^{j+i\alpha}}) \mid \theta(x^{c^i})$ in $\mathbb{C}[x]$. Moreover, noting that $T_{b^k}(x^{b^{j+i\alpha}}) \in \mathbb{Z}[x]$ is monic, we immediately conclude that $T_{b^k}(x^{b^{j+i\alpha}}) \mid \theta(x^{c^i})$ in $\mathbb{Z}[x]$.

(ii) Suppose that η belongs to $\mathrm{Root}(T_{b^k}(x^{b^j})) \cap \mathrm{Root}(\theta(x^{c^i}))$. Repeating the same argument as in (i), we derive from $\eta \in \mathrm{Root}(T_{b^k}(x^{b^j}))$ that $\eta^c \in \mathrm{Root}(T_{b^k}(x^{b^{j-\alpha}}))$. On the other hand, $\eta \in \mathrm{Root}(\theta(x^{c^i}))$ gives $\eta^c \in \mathrm{Root}(\theta(x^{c^{i-1}}))$. Therefore, $\eta^c \in \mathrm{Root}(T_{b^k}(x^{b^{j-\alpha}})) \cap \mathrm{Root}(\theta(x^{c^{i-1}}))$. □

3. Order, shifting parameter, and Hall polynomial

In this section, we work on the relationship among the order n, the shifting parameter g, and the Hall polynomial $\theta_A(x)$ of any (0, 1) g-circulant solution A to $A^m = J_n$ by analyzing the root sets of related polynomials. The following theorem is a long step towards achieving our objective.

Theorem 3.1. *Let c, n be two natural numbers with $c \mid n$ and $c = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, where p_i, $1 \leqslant i \leqslant s$, are distinct primes and $\alpha_i \in \mathbb{N}$. Let $1 \neq m \in \mathbb{N}$. If $\theta(x) \in \mathbb{Z}^*[x]$ satisfies that $\prod_{i=0}^{m-1} \theta(x^{c^i}) \equiv T_n(x) \pmod{x^n - 1}$, then there exist $k_i \in \mathbb{N}$ for each i, $1 \leqslant i \leqslant s$, such that $\theta(1) = p_1^{\alpha_1 k_1} p_2^{\alpha_2 k_2} \cdots p_s^{\alpha_s k_s}$, $n = (\theta(1))^m = p_1^{m\alpha_1 k_1} p_2^{m\alpha_2 k_2} \cdots p_s^{m\alpha_s k_s}$, and $\prod_{i=1}^{s} \Phi_{p_i^{\alpha_i}, k_i, m}(x) \mid \theta(x)$.*

Proof. It is obvious that $n = (\theta(1))^m$. So we turn to consider the remaining claims.

For any prime p with $(p, c) = 1$, by letting $\alpha = 0$, $k = 1$, $j = 0$, $b = p$, and noting the irreducibility of $T_p(x)$ over Q, we deduce from Lemma 2.9 that either $T_p(x)$ divides $\theta(x^{c^i})$ for all $i \in \mathbb{Z}^*$ or $T_p(x)$ does not divide $\theta(x^{c^i})$ for all $i \in \mathbb{Z}^*$. This shows that $T_p(x)$ is a factor of $\prod_{i=0}^{m-1} \theta(x^{c^i})$ with multiplicity 0 or at least $m > 1$. But we also know from Lemmas 2.4 and 2.7 that, for any divisor p of n, $T_p(x)$ is a factor of $\prod_{i=0}^{m-1} \theta(x^{c^i})$ with multiplicity exactly 1. This tells us that all divisors of n must be divisors of c too.

Let p be a prime factor of c and $\alpha = \mathrm{ord}_p(c) > 0$. Write $\mathrm{ord}_p(n) = k\alpha m + \beta$, where $k \in \mathbb{N}$ and $0 \leqslant \beta < \alpha m$.

If it holds that $T_{p^\alpha}(x^{p^{j\alpha m}}) \mid \theta(x)$ for all j, $0 \leqslant j \leqslant k$, then Lemma 2.9(i) implies

$$T_{p^\alpha}\left(x^{p^{(jm+i)\alpha}}\right) \mid \theta\left(x^{c^i}\right)$$

for $0 \leqslant j \leqslant k$ and $0 \leqslant i \leqslant m - 1$. Making use of the fact that these polynomials $T_{p^\alpha}(x^{p^{(jm+i)\alpha}})$, where $0 \leqslant j \leqslant k$ and $0 \leqslant i \leqslant m - 1$, are pairwise prime, we conclude that $\prod_{l=0}^{(k+1)m-1} T_{p^\alpha}(x^{p^{l\alpha}}) \mid \prod_{i=0}^{m-1} \theta(x^{c^i})$ in $\mathbb{Z}[x]$. Putting $x = 1$ in this relation, we see that $p^{\alpha(k+1)m} \mid (\theta(1))^m$, which contradicts the fact $n = (\theta(1))^m$ and $\mathrm{ord}_p(n) < \alpha(k + 1)m$. Therefore, we can take an integer j, $0 \leqslant j \leqslant k$, for which

$$T_{p^\alpha}\left(x^{p^{j\alpha m}}\right) \nmid \theta(x). \tag{5}$$

Choose σ to be the smallest one among all such j's. Then we clearly have $\mathrm{ord}_p(n) - \sigma\alpha m \in \mathbb{Z}^*$. Let us use δ for the nonnegative integer $\min\{\mathrm{ord}_p(n) - \sigma\alpha m, \alpha\}$.

Since $c \mid n$, Lemma 2.8 asserts $T_{p^\alpha}(x) \mid \theta(x)$. Hence $\sigma \geqslant 1$. The choice of σ guarantees that $T_{p^\alpha}(x^{p^{l\alpha m}}) \mid \theta(x)$ for $l = 0, 1, \ldots, \sigma - 1$. Thus, by Lemma 2.9(i), we have

$$T_{p^\alpha}\bigl(x^{p^{(lm+i)\alpha}}\bigr) \bigm| \theta\bigl(x^{c^i}\bigr) \quad \text{in } \mathbb{Z}[x] \tag{6}$$

for $0 \leqslant l \leqslant \sigma - 1,\ i \in \mathbb{Z}^*$.

Note that Lemma 2.2 says $T_{p^\alpha}(x^{p^{lm\alpha}})$ are pairwise prime for $0 \leqslant l \leqslant \sigma - 1$. So by letting $i = 0$ in (6) we have

$$\Phi_{p^\alpha,\sigma,m}(x) \mid \theta(x). \tag{7}$$

Another consequence of (6), which we will make use of later, is obtained by substituting $l = \sigma - 1$ and $i = m - 1$ into it:

$$\operatorname{Root}\bigl(T_{p^\alpha}\bigl(x^{p^{(\sigma m-1)\alpha}}\bigr)\bigr) \subseteq \operatorname{Root}\bigl(\theta\bigl(x^{c^{m-1}}\bigr)\bigr). \tag{8}$$

From $\sigma m\alpha + \delta \leqslant \operatorname{ord}_p(n)$, we know that $T_{p^\delta}(x^{p^{\sigma\alpha m}}) \mid T_n(x)$. But $\prod_{i=0}^{m-1} \theta(x^{c^i}) \equiv T_n(x) \pmod{x^n - 1}$ shows that $T_n(x) \mid \prod_{i=0}^{m-1} \theta(x^{c^i})$. Hence, we get

$$\operatorname{Root}\left(T_{p^\delta}\left(x^{p^{\sigma\alpha m}}\right)\right) \subseteq \operatorname{Root}\left(\prod_{i=0}^{m-1} \theta\bigl(x^{c^i}\bigr)\right). \tag{9}$$

If there exists $\gamma \in \{1, 2, \ldots, m-1\}$ with $\operatorname{Root}(T_{p^\delta}(x^{p^{\sigma\alpha m}})) \cap \operatorname{Root}(\theta(x^{c^\gamma})) \neq \emptyset$, then Lemma 2.9(ii) would imply

$$\operatorname{Root}\bigl(T_{p^\delta}\bigl(x^{p^{(\sigma m-1)\alpha}}\bigr)\bigr) \cap \operatorname{Root}\bigl(\theta\bigl(x^{c^{\gamma-1}}\bigr)\bigr) \neq \emptyset. \tag{10}$$

Note that $\delta \leqslant \alpha$ gives

$$\operatorname{Root}\bigl(T_{p^\delta}\bigl(x^{p^{(\sigma m-1)\alpha}}\bigr)\bigr) \subseteq \operatorname{Root}\bigl(T_{p^\alpha}\bigl(x^{p^{(\sigma m-1)\alpha}}\bigr)\bigr),$$

and hence (8) implies

$$\operatorname{Root}\bigl(T_{p^\delta}\bigl(x^{p^{(\sigma m-1)\alpha}}\bigr)\bigr) \subseteq \operatorname{Root}\bigl(\theta\bigl(x^{c^{m-1}}\bigr)\bigr). \tag{11}$$

At this point, since $\gamma - 1 < m - 1$, we can combine (10) and (11) to deduce that $\prod_{i=0}^{m-1} \theta(x^{c^i})$ has a multiple root which is a root of unity and whose order is a prime power. This violates Lemma 2.7, since, by Lemma 2.4, $\prod_{i=0}^{m-1} \theta(x^{c^i}) \in F_n$. So, we conclude from (9) that $\operatorname{Root}(T_{p^\delta}(x^{p^{\sigma\alpha m}})) \subseteq \operatorname{Root}(\theta(x))$.

Invoking Lemma 2.9(i) again, we obtain

$$T_{p^\delta}\bigl(x^{p^{(\sigma m+i)\alpha}}\bigr) \mid \theta(x^{c^i}) \text{ in } \mathbb{Z}[x] \tag{12}$$

for $0 \leqslant i \leqslant m - 1$. So we see that $\delta < \alpha$, as otherwise it would follow from (12) (by putting $i = 0$) that $T_{p^\alpha}(x^{p^{\sigma\alpha m}}) \mid \theta(x)$ in $\mathbb{Z}[x]$, contradicting (5). It is readily seen from $\delta = \min\{\operatorname{ord}_p(n) - \sigma\alpha m, \alpha\}$ that

$$k = \sigma \tag{13}$$

and $\delta = \beta$.

Noting that all the polynomials T's which appear in (6) or (12) are pairwise prime, we conclude that

$$\left(\prod_{i=0}^{km-1} T_{p^\alpha}\left(x^{p^{i\alpha}}\right)\right)\left(\prod_{i=0}^{m-1} T_{p^\beta}\left(x^{p^{(km+i)\alpha}}\right)\right)\Bigg|\prod_{i=0}^{m-1}\theta\left(x^{c^i}\right)$$

in $\mathbb{Z}[x]$. Setting $x=1$, we obtain $p^{k\alpha m+\beta m}|n$. Observe that $\mathrm{ord}_p(n)=k\alpha m+\beta$. So it must hold that $\beta m \leqslant \beta$. But we have $m \geqslant 2$ and $\beta \geqslant 0$. This is possible only if $\beta = 0$, that is, $\mathrm{ord}_p(n)=k\alpha m$. It then follows from $n=(\theta(1))^m$ that $\mathrm{ord}_p(\theta(1))=k\alpha$. Moreover, since $\sigma = k$, (7) gives $\Phi_{p^\alpha,k,m}(x)\,|\,\theta(x)$.

Applying the above argument to each p_i, $1 \leqslant i \leqslant s$, we obtain a corresponding $k_i \in \mathbb{N}$ such that $\mathrm{ord}_{p_i}(\theta(1)) = k_i\alpha_i$ and $\Phi_{p_i^{\alpha_i},k_i,m}(x)\,|\,\theta(x)$. Hence we get $\theta(1) = p_1^{\alpha_1 k_1}p_2^{\alpha_2 k_2}\cdots p_s^{\alpha_s k_s}$, as required. Further noticing that $\Phi_{p_i^{\alpha_i},k_i,m}(x)$, $i=1,\ldots,s$, are pairwise prime (see Lemma 2.2), we then obtain $\prod_{i=1}^s \Phi_{p_i^{\alpha_i},k_i,m}(x)\,|\,\theta(x)$ and thus complete the proof. □

Our next theorem summarizes what we have known about the relations among the three parameters g, n and $\theta_A(x)$ for a (0, 1) g-circulant solution A to Eq. (1). As a matter of fact, it says a bit more.

Theorem 3.2. *Let g, n be natural numbers for which $c=(g,n)$ has a factorization $c=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, where p_i, $1 \leqslant i \leqslant s$, are distinct primes and $\alpha_i \in \mathbb{N}$. Assume that a* (0, 1) *g-circulant A satisfies $A^m = J_n$. Then*:

(i) *$T_c(x)\,|\,\theta(x)$.*
(ii) *There exist $k_i \in \mathbb{N}$, $1 \leqslant i \leqslant s$, such that $\theta(1)=\prod_{i=1}^s p_i^{\alpha_i k_i}$ and $n=\theta(1)^m=\prod_{i=1}^s p_i^{m\alpha_i k_i}$.*
(iii) *$\prod_{i=1}^s \Phi_{p_i^{\alpha_i},k_i,m}(x)\,|\,\theta(x)$.*
(iv) *$(g/c, n) = 1$.*
(v) *If a positive divisor l of n satisfies*:
  (a) *for some $i \in \{1,2,\ldots,s\}$, there exists an $f \in \mathbb{N}$ such that $\mathrm{ord}_{p_i}(l) \in \{\alpha_i fm+1, \alpha_i fm+2, \ldots, \alpha_i fm+\alpha_i\}$ (note that we have in fact $f \in \{1,2,\ldots,k_i-1\}$ since $l\,|\,n$) and*
  (b) *$\mathrm{ord}_{p_j}(l) \in \{0,1,\ldots,\alpha_j\}$ if $j \neq i$,*
  then $\phi_l(x)\,|\,\theta(x)$.

Proof. By Theorem 1.2, we have

$$\prod_{i=0}^{m-1}\theta\left(x^{c^i}\right) \equiv T_n(x) \pmod{x^n-1}. \qquad (14)$$

Hence the first three claims follow from Lemma 2.8 and Theorem 3.1, respectively. So our task is to prove (iv) and (v).

We first give the argument for (iv). Observe that each prime factor of n is also a factor of n/c due to the fact that $n = \prod_{i=1}^{s} p_i^{m\alpha_i k_i}$, $c = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, and $m \geqslant 2$. But $(g/c, n/c) = 1$. It then follows that $(g/c, n) = 1$.

Now we are proving (v). From $l \mid n$ and (14), we deduce that

$$\mathrm{Root}(\phi_l(x)) \subseteq \bigcup_{i=0}^{m-1} \mathrm{Root}\big(\theta(x^{c^i})\big).$$

Observe that our assertion $\phi_l(x) \mid \theta(x)$ is equivalent to $\mathrm{Root}(\phi_l(x)) \subseteq \mathrm{Root}(\theta(x))$. Therefore, in order to establish (iv) it suffices to show that $\mathrm{Root}(\phi_l(x)) \cap \mathrm{Root}(\theta(x^{c^v})) = \emptyset$ for $v = 1, 2, \ldots, m-1$. We will do this by way of contradiction and hence complete the proof.

Assume that there is an integer $v \in \{1, 2, \ldots, m-1\}$ such that there exists some number $\xi \in \mathrm{Root}(\phi_l(x)) \cap \mathrm{Root}(\theta(x^{c^v}))$. Let $\eta = \xi^c$. Then $\xi \in \mathrm{Root}(\phi_l(x))$ implies η is a root of unity whose order is $l/(l, c)$. But (a) together with (b) shows that there is some $w \in \{\alpha_i((f-1)m + m - 1) + 1, \alpha_i((f-1)m + m - 1) + 2, \ldots, \alpha_i((f-1)m + m - 1) + \alpha_i\}$ such that $l/(l, c) = p_i^w$. So, in virtue of $f \in \{1, 2, \ldots, k_i - 1\}$, (6) and (13) tell us that $\eta \in \mathrm{Root}(\theta(x^{c^{m-1}}))$. Going the other way, since $\xi \in \mathrm{Root}(\theta(x^{c^v}))$, we have $\eta = \xi^c \in \mathrm{Root}(\theta(x^{c^{v-1}}))$. However, $v - 1 < m - 1$, and thus η is a multiple root of $\prod_{i=0}^{m-1} \theta(x^{c^i}) = 0$, contradicting Lemmas 2.4 and 2.7. □

Using Theorem 3.1, we can give a characterization of all the g-circulant solutions to $A^m = J_n$ for n being a prime power in the ensuing result. We remark that it was also obtained independently by Wang [30].

Theorem 3.3. *Suppose that A is a g-circulant and $n \in \mathbb{N}$ is a prime power. Let $c = (g, n)$ and $r = \theta_A(1)$. Then $A^m = J_n$ if and only if the following hold*:
(i) $n = r^m$.
(ii) *There exists $k \in \mathbb{N}$ such that $r = c^k$ and $\Phi_{c,k,m}(x) \mid \theta_A(x)$.*

Proof. The “if” part follows immediately from Lemma 2.3 while the “only if” part is a direct consequence of Theorem 3.1. □

Another application of Theorem 3.1 leads to a complete determination of all the (0, 1) g-circulant solutions to Eq. (1) when $\mathrm{ord}_p n = m$ for each prime factor p of n. But we defer this treatment to Section 6, since we can say something more about this case there.

4. $\Omega'_{c,k,m}$ and $\Omega_{c,k,m}$

For $c, k, m \in \mathbb{N}$, we define $\Omega'_{c,k,m}$ to be the set of polynomials $f(x) \in \mathbb{Z}^*[x]$ with $\Phi_{c,k,m}(x) \mid f(x)$ and $f(1) = c^k$. In view of Lemma 2.3, we see that each member of $\Omega'_{c,k,m}$ is in fact a (0, 1) polynomial. Often we put a restriction on the degree of the polynomials in our consideration due to the fact that the Hall polynomial of a g-circulant of size $n \times n$ has degree less than n. Here we denote by $\Omega_{c,k,m}$ the set consisting of those members of $\Omega'_{c,k,m}$ which have degree less than c^{km}. Note that if Wang's conjecture is correct, then in order to enumerate all (0, 1) g-circulant solutions A to Eq. (1) it is sufficient to enumerate all elements in $\Omega_{c,k,m}$ for which $c^{km} = n$. Note also that Theorem 3.1 means that if a (0, 1) g-circulant A satisfies $A^m = J_n$, then for each prime factor p of n we have $\mathrm{ord}_p(n) = \alpha km$ for some natural numbers α and k, and $\theta_A(x) \in \Omega'_{p^\alpha,k,m}$. The next result identifies $\Omega'_{c,k,m}$ and $\Omega_{c,k,m}$ by explicitly formulating their members. We have known that Wang also succeeded in determining $\Omega_{c,k,m}$ for any prime power c using a different approach [30,31].

Theorem 4.1.

(i) $\Omega'_{c,k,m}$ *consists of the polynomials*

$$\sum_{i_1=0}^{c-1}\sum_{i_2=0}^{c-1}\cdots\sum_{i_k=0}^{c-1} x^{\sum_{j=1}^{k} p_{i_1,i_2,\ldots,i_j} c^{(j-1)m+1} + \sum_{j=1}^{k} i_j c^{(j-1)m}}, \tag{15}$$

where the p*'s with fewer than* k *subscripts take values in* $\{0, 1, \ldots, c^{m-1} - 1\}$ *while the* p*'s with* k *subscripts take values in* $\mathbb{Z}^*$.

(ii) $\Omega_{c,k,m}$ *consists of the polynomials*

$$\sum_{i_1=0}^{c-1}\sum_{i_2=0}^{c-1}\cdots\sum_{i_k=0}^{c-1} x^{\sum_{j=1}^{k} p_{i_1,i_2,\ldots,i_j} c^{(j-1)m+1} + \sum_{j=1}^{k} i_j c^{(j-1)m}}, \tag{16}$$

where all p*'s take values in* $\{0, 1, \ldots, c^{m-1} - 1\}$.

Proof. We first claim that any member in $\Omega'_{c,k,m}$ can be represented as in (15) and any member in $\Omega_{c,k,m}$ can be represented as in (16).

We proceed by using induction on k to establish the results for both $\Omega'_{c,k,m}$ and $\Omega_{c,k,m}$ simultaneously. For $k = 1$, since $\Phi_{c,1,m}(x)$ is just $T_c(x)$, it is not difficult to check that the assertion follows from Corollary 2.1. So let us assume that the assertion holds for $k = t - 1$ and turn to consider the case $k = t \geqslant 2$.

Let $f(x) \in \Omega'_{c,t,m}$. Set $s = c^{(t-1)m}$ and define $g(x) = \sum_{j=0}^{s-1} (f_{j,s}(1)/c)x^j$. By the definition of $\Omega'_{c,t,m}$, we have $T_c(x^s) \mid f(x)$. So we can apply Lemma 2.1(iii) to get $g(x) \in \mathbb{Z}^*[x]$. By Lemma 2.1(ii), we have

$$\begin{aligned} f(x) &= \sum_{j=0}^{s-1} f_{j,s}(x) \\ &\equiv \sum_{j=0}^{s-1} (f_{j,s}(1)/c)x^j T_c(x^s) \pmod{x^{cs} - 1}. \end{aligned}$$

This is just

$$f(x) \equiv T_c(x^s)g(x) \pmod{x^{cs}-1}. \tag{17}$$

Note that $\Phi_{c,t,m}(x) \mid (f(x), x^{cs}-1)$. Hence (17) shows $\Phi_{c,t,m}(x) \mid T_c(x^s)g(x)$, which implies $\Phi_{c,t-1,m}(x) \mid g(x)$. Furthermore, we have $\deg g(x) < s$ and $g(1) = f(1)/c = c^{t-1}$. Thus we arrive at $g(x) \in \Omega_{c,t-1,m}$ and henceforth our induction hypothesis asserts now there are some p's falling into the set $\{0, 1, \ldots, c^{m-1}-1\}$ and

$$g(x) = \sum_{i_1=0}^{c-1}\sum_{i_2=0}^{c-1}\cdots\sum_{i_{t-1}=0}^{c-1} x^{\sum_{j=1}^{t-1} p_{i_1,i_2,\ldots,i_j} c^{(j-1)m+1} + \sum_{j=1}^{t-1} i_j c^{(j-1)m}}. \tag{18}$$

In view of Lemma 2.3, $g(x)$ is a (0, 1) polynomial, which means $f_{j,s}(1)$ can only take values 0 and c when j runs from 0 to $s-1$. For any polynomial $h(x) = \sum_{j=0}^{n-1} h_j x^j$, we define $X(h(x))$ to be the set $\{j : 0 \leqslant j \leqslant n-1, h_j \neq 0\}$. In terms of this notation, we have

$$X(g(x)) = \left\{ \sum_{j=1}^{t-1} p_{i_1,i_2,\ldots,i_j} c^{(j-1)m+1} + \sum_{j=1}^{t-1} i_j c^{(j-1)m} : i_j = 0, 1, \ldots, c-1, \right. \\ \left. j = 1, 2, \ldots, t-1 \right\}$$

and $|X(g(x))| = c^{t-1}$.

Using Lemma 2.1(iv), we know that for each j with $f_{j,s}(1) = c$, it holds

$$f_{j,s}(x) = x^j \sum_{i_t=0}^{c-1} x^{u_{j,i_t} cs + i_t s} \tag{19}$$

for some nonnegative integers u_{j,i_t}, $i_t = 0, 1, \ldots, c-1$. In the following, we shall write $p_{i_1,i_2,\ldots,i_t}$ for u_{j,i_t} provided that

$$j = \sum_{q=1}^{t-1} p_{i_1,i_2,\ldots,i_q} c^{(q-1)m+1} + \sum_{q=1}^{t-1} i_q c^{(q-1)m}.$$

Recalling the definition of $g(x)$, we derive the following formula from the combination of Lemma 2.1(v), (18), and (19):

$$\begin{aligned} f(x) &= \sum_{\substack{0 \leqslant q \leqslant s-1 \\ f_{q,s}(1)=c}} f_{q,s}(x) \\ &= \sum_{q \in X(g(x))} f_{q,s}(x) \end{aligned}$$

$$\begin{aligned}
&= \sum_{q\in X(g(x))} x^{q}\left(\sum_{i_t=0}^{c-1} x^{u_{q,i_t}cs+i_t s}\right)\\
&= \sum_{i_1=0}^{c-1}\sum_{i_2=0}^{c-1}\cdots\sum_{i_{t-1}=0}^{c-1}\left(x^{\sum_{j=1}^{t-1} p_{i_1,i_2,\ldots,i_j}c^{(j-1)m+1}+\sum_{j=1}^{t-1} i_j c^{(j-1)m}}\right.\\
&\qquad\qquad\left.\times\left(\sum_{i_t=0}^{c-1} x^{p_{i_1,i_2,\ldots,i_t}cs+i_t s}\right)\right)\\
&= \sum_{i_1=0}^{c-1}\sum_{i_2=0}^{c-1}\cdots\sum_{i_t=0}^{c-1} x^{\sum_{j=1}^{t} p_{i_1,i_2,\ldots,i_j}c^{(j-1)m+1}+\sum_{j=1}^{t} i_j c^{(j-1)m}}. \qquad (20)
\end{aligned}$$

Clearly (20) means each member $f(x)$ of $\Omega'_{c,t,m}$ can be represented as in (15) when $k=t$. If $f(x)$ is also a member of $\Omega_{c,t,m}$, that is, $\deg f(x) \leqslant c^{tm}$, it is easy to see that this assumption poses a restriction on $p_{i_1,i_2,\ldots,i_{t-1},i_t}$, where $i_j \in \{0,1,\ldots,c-1\}$, $j=1,2,\ldots,t$, namely they cannot exceed $c^{m-1}-1$. Hence it also follows that it has an expression as in (16) in case of $k=t$. So, by principle of induction, our first claim is reached.

Next, we shall show that all polynomials expressed as in (15) and (16) are members of $\Omega'_{c,k,m}$ and $\Omega_{c,k,m}$, respectively.

In fact, by letting $\sigma_{i_1,\ldots,i_{k-1}} = \sum_{j=1}^{k-1} p_{i_1,i_2,\ldots,i_j}c^{(j-1)m+1} + \sum_{j=1}^{k-1} i_j c^{(j-1)m}$, we have

$$\begin{aligned}
&\sum_{i_1=0}^{c-1}\sum_{i_2=0}^{c-1}\cdots\sum_{i_k=0}^{c-1} x^{\sum_{j=1}^{k} p_{i_1,i_2,\ldots,i_j}c^{(j-1)m+1}+\sum_{j=1}^{k} i_j c^{(j-1)m}}\\
&\quad= \sum_{i_1=0}^{c-1}\sum_{i_2=0}^{c-1}\cdots\sum_{i_{k-1}=0}^{c-1}\left(x^{\sigma_{i_1,\ldots,i_{k-1}}}\sum_{i_k=0}^{c-1} x^{p_{i_1,i_2,\ldots,i_k}c^{(k-1)m+1}+i_k c^{(k-1)m}}\right)\\
&\quad= \sum_{i_1=0}^{c-1}\sum_{i_2=0}^{c-1}\cdots\sum_{i_{k-1}=0}^{c-1}\left(x^{\sigma_{i_1,\ldots,i_{k-1}}}\sum_{i_k=0}^{c-1} x^{i_k c^{(k-1)m}}\right)\\
&\qquad+ \sum_{i_1=0}^{c-1}\sum_{i_2=0}^{c-1}\cdots\sum_{i_{k-1}=0}^{c-1}\left(x^{\sigma_{i_1,\ldots,i_{k-1}}}\sum_{i_k=0}^{c-1}\left(x^{p_{i_1,i_2,\ldots,i_k}c^{(k-1)m+1}}-1\right)x^{i_k c^{(k-1)m}}\right)\\
&\quad\equiv T_c\left(x^{c^{(k-1)m}}\right)\sum_{i_1=0}^{c-1}\sum_{i_2=0}^{c-1}\cdots\sum_{i_{k-1}=0}^{c-1} x^{\sigma_{i_1,\ldots,i_{k-1}}} \quad \left(\operatorname{mod} x^{c^{(k-1)m+1}}-1\right).
\end{aligned}$$

Thus, by applying induction on k, we can show that the polynomials represented in (15) or (16) are divisible by $\Phi_{c,k,m}(x)$. But all these polynomials have nonnegative coefficients summing to c^k. Therefore, they belong to $\Omega'_{c,k,m}$. Furthermore, it is clear that each polynomial represented in (16) is of degree less than c^{km} and hence is in $\Omega_{c,k,m}$. This completes the proof. □

From the expression of $\Omega_{c,k,m}$, its cardinality can be easily obtained.

Theorem 4.2. $|\Omega_{c,k,m}| = c^{(m-1)c(c^k-1)/(c-1)}$.

Proof. Note that in (15) the number of p's with r subscripts is c^r. So, there are altogether $\sum_{i=1}^{k} c^i = c(c^k - 1)/(c - 1)$ p's in (15), each of which takes value from $\{0, 1, 2, \ldots, c^{m-1} - 1\}$. Thus the theorem follows. □

We conclude this section by giving an equivalent statement of Theorem 4.2 in terms of addition set. We are still not sure if the Hall polynomial of any planar (c^{km}, c^k, m)-addition set must be divisible by $\Phi_{c,k,m}(x)$. Of course, our results in last section say that this is indeed the case if n is a prime power or if c^k is square-free, and hence in such cases the assumption on Hall polynomial in the following theorem is redundant.

Theorem 4.3. *Let c, r, k, n be positive integers such that $r = c^k$ and $n = r^m$. Then the total number of planar (n, r, m)-addition sets with their Hall polynomial divisible by $\Phi_{c,k,m}(x)$ is $c^{(m-1)c(c^k-1)/(c-1)}$.*

5. Shifting parameter against Hall polynomial

In this section, we consider the class of g-circulant solutions to $A^m = J_n$, whose Hall polynomials are divisible by some polynomial $\Phi_{c,k,m}(x)$ or, more generally, just by $T_c(x)$. More precisely, we will examine how the shifting parameters of such g-circulant solutions behave. Our work here develops the technique in [3], where Chao and Wang have shown that if a (0, 1) g-circulant A satisfies $A^2 = J$, $\theta_A(1) = c$, and $T_c(x) \mid \theta_A(x)$, then there exists $t \in \mathbb{N}$ such that $g = ct$ and $(t, c) = 1$.

Theorem 5.1. *Let A be a g-circulant solution to $A^m = J_n$.*
(i) *If $T_c(x) \mid \theta_A(x)$, then there exists $t \in \mathbb{N}$ such that $g = ct$.*
(ii) *Suppose $\theta_A(1) = c^k$ and $\Phi_{c,k,m}(x) \mid \theta_A(x)$. Then there exists $t \in \mathbb{N}$ such that $g = ct$ and $(t, c) = 1$.*

Proof. (i) Let $d = (g, c)$, $c = hd$ and $g = ed$. Then $(e, h) = 1$ and there exists $f \in \mathbb{Z}$ such that $ef \equiv 1 \pmod h$.

Our aim is to show that $c \mid d$.

Let $\theta(x) = \sum_{i=0}^{r-1} x^{\alpha_i}$ be the Hall polynomial of A and $X = X(\theta(x)) = \{\alpha_i : 0 \leqslant i \leqslant r - 1\}$. Clearly $r = \theta(1)$.

To make our argument not too lengthy, we will use the following notations:

$$S_i = \{b\colon\ b \in X,\ b \equiv i \pmod h\},$$

$$R_i = \{b\colon\ b \in X, b \equiv id \pmod c\},$$

$$T_i = \left\{(b_1, b_2, \ldots, b_{m-1}) : b_j \in X,\ 1 \leqslant j \leqslant m-1, \right.$$
$$\left. \sum_{j=1}^{m-1} b_j g^j \equiv id \pmod c\right\},$$

$$W_i = \left\{(b_0, b_1, \ldots, b_{m-1}) : b_j \in X,\ 0 \leqslant i \leqslant m-1, \right.$$
$$\left. \sum_{j=0}^{m-1} b_j g^j \equiv id \pmod c\right\},$$

$$\Sigma_i = \sum_{(b_0,b_1,\ldots,b_{m-1})\in W_i} \sum_{j=0}^{m-1} b_j g^j.$$

Note that for any $(b_0, b_1, \ldots, b_{m-1}) \in W_i$, it follows from $d = (g, c)$ that $d \mid b_0$. Hence we have

$$\Sigma_i = \Sigma_i^1 + \Sigma_i^2, \tag{21}$$

where

$$\Sigma_i^1 = \sum_{p=0}^{h-1} \left(|T_{i-p}| \sum_{b_0\in R_p} b_0 \right),$$

and

$$\Sigma_i^2 = \sum_{p=0}^{h-1} \left(|R_p| \sum_{(b_1,b_2,\ldots,b_{m-1})\in T_{i-p}} \sum_{j=1}^{m-1} b_j g^j \right).$$

Since $T_c(x) \mid \theta(x)$, we know from Lemma 2.1(ii) that $|R_p| = r/c$ for all p. This enables us to write

$$\begin{aligned}\Sigma_i^2 &= (r/c) \left(\sum_{p=0}^{h-1} \sum_{(b_1,b_2,\ldots,b_{m-1})\in T_{i-p}} \sum_{j=1}^{m-1} b_j g^j \right)\\ &= (r/c) \left(\sum_{p=0}^{h-1} \sum_{(b_1,b_2,\ldots,b_{m-1})\in T_p} \sum_{j=1}^{m-1} b_j g^j \right).\end{aligned} \tag{22}$$

Note that $T_h(x) \mid T_c(x)$ and thus by invoking Lemma 2.1(ii) again, our hypothesis $T_c(x) \mid \theta(x)$ leads to the assertion $|S_p| = r/h$ for all p. Therefore, for any $j \in \mathbb{Z}$, we have

$$\begin{aligned}
\left|T_j\right| &= \left|\left\{(b_1, b_2, \cdots, b_{m-1}) : b_l \in X,\ 1 \leqslant l \leqslant m-1,\right.\right.\\
&\qquad \left.\left.\sum_{l=1}^{m-1} b_l g^l \equiv jd \pmod{c}\right\}\right|\\
&= \left|\left\{(b_1, b_2, \ldots, b_{m-1}) : b_l \in X,\ 1 \leqslant l \leqslant m-1,\right.\right.\\
&\qquad \left.\left.e\sum_{l=1}^{m-1} b_l g^{l-1} \equiv j \pmod{h}\right\}\right|\\
&= \left|\left\{(b_1, b_2, \ldots, b_{m-1}) : b_l \in X,\ 1 \leqslant l \leqslant m-1,\right.\right.\\
&\qquad \left.\left.\sum_{l=1}^{m-1} b_l g^{l-1} \equiv fj \pmod{h}\right\}\right|\\
&= (r/h)^{m-1}\left|\left\{(b_1, b_2, \ldots, b_{m-1}) : 0 \leqslant b_l \leqslant h-1,\ 1 \leqslant l \leqslant m-1,\right.\right.\\
&\qquad \left.\left.\sum_{l=1}^{m-1} b_l g^{l-1} \equiv fj \pmod{h}\right\}\right|\\
&= (r/h)^{m-1}\sum_{b_1=0}^{h-1}\left|\left\{(b_1, b_2, \ldots, b_{m-1}) : 0 \leqslant b_l \leqslant h-1, 2 \leqslant l \leqslant m-1,\right.\right.\\
&\qquad \left.\left.\sum_{l=2}^{m-1} b_l g^{l-1} \equiv fj - b_1 \pmod{h}\right\}\right|\\
&= (r/h)^{m-1}\sum_{b=0}^{h-1}\left|\left\{(b_1, b_2, \ldots, b_{m-1}) : 0 \leqslant b_l \leqslant h-1, 2 \leqslant l \leqslant m-1,\right.\right.\\
&\qquad \left.\left.\sum_{l=2}^{m-1} b_l g^{l-1} \equiv b \pmod{h}\right\}\right|. \qquad (23)
\end{aligned}$$

The last equality is due to the fact that if b_1 ranges over a complete representative system of residues modulo h, then so is $fj - b_1$. Since the parameter j does not appear in formula (23), we see that there is a number τ such that $|T_j| = \tau$ for all j. So we obtain the following expression for Σ_i^1:

$$\Sigma_i^1 = \tau \sum_{p=0}^{h-1} \sum_{b_0 \in R_p} b_0. \tag{24}$$

Combining (22) and (24) we know that Σ_i is in fact independent of the parameter i. In particular, we have

$$0 = \Sigma_0 - \Sigma_1.$$

But as $A^m = J_n$, Theorem 1.3 says that

$$\Sigma_0 \equiv \sum_{i=0}^{n/c-1} ic \pmod n$$

and

$$\Sigma_1 \equiv \sum_{i=0}^{n/c-1} (ic+d) \pmod n.$$

Hence we get $0 \equiv dn/c \pmod n$ and thus it follows $c \mid d$, as desired.

(ii) Owing to (i) and that $T_c(x) \mid \Phi_{c,k,m}(x)$, our work is reduced to showing $(c,t) = 1$. Note that we have now $\deg \theta(x) < n$, $\theta(1) = c^k$ and $\Phi_{c,k,m}(x) \mid \theta(x)$, which is just equivalent to saying that $\theta(x)$ is in the class $\Omega_{c,k,m}$, since $n = \theta(1)^m = c^{km}$. By Theorem 4.1, there are some p's taking values in $\{0, 1, \ldots, c^{m-1} - 1\}$ such that

$$X = \left\{ \sum_{j=1}^{k} p_{i_1,i_2,\ldots,i_j} c^{(j-1)m+1} \right. \\ \left. + \sum_{j=1}^{k} i_j c^{(j-1)m} : i_j = 0, 1, \ldots, c-1, j = 1, 2, \ldots, k \right\}.$$

Let $q = (c,t)$. Suppose that the assertion $(c,t) = 1$ is false. Then $1 \leqslant c/q < c$. Let γ_1 and γ_2 be the two integers in X which correspond to $i_j = 0,\ 0 \leqslant j \leqslant k$, and $i_j = 0,\ 0 \leqslant j \leqslant k-1,\ i_k = c/q$, respectively, that is,

$$\gamma_1 = p_0 c + p_{0,0} c^{m+1} + \cdots + p_{\underbrace{0,0,\ldots,0}_{k \text{ zeros}}} c^{(k-1)m+1},$$

$$\gamma_2 = p_0 c + p_{0,0} c^{m+1} + \cdots + p_{\underbrace{0,0,\ldots,0}_{k-1 \text{ zeros}},c/q} c^{(k-1)m+1} + (c/q) c^{(k-1)m}.$$

It is easily verified that

$$\gamma_1 + \gamma_1 g^2 + \cdots + \gamma_1 g^{m-1} \\ \equiv \gamma_1 + \gamma_1 g^2 + \cdots + \gamma_1 g^{m-2} + \gamma_2 g^{m-1} \pmod{c^{km}},$$

which contradicts Theorem 1.3, since it holds $n = c^{km}$ here. This contradiction concludes the proof of the theorem. □

We remark that Theorem 5.1(i) can be viewed as a converse of Lemma 2.8, while Theorem 5.1(ii) illustrates that $P_{c,k,m}$ is just the set of (0, 1) g-circulant solutions A to $A^m = J_{c^{km}}$ with $\Phi_{c,k,m}(x) \mid \theta_A(x)$.

6. Isomorphism

In this section, we study the isomorphism relations among solutions to $A^m = J_n$. Throughout this section, all the computations involving integer addition and multiplication are implicitly executed modulo n.

Our first goal is to show that in some cases the g-circulant solution to $A^m = J_n$ is unique up to isomorphism. For this purpose one lemma is needed.

Lemma 6.1. *Let A be a g-circulant solution to $A^m = J_n$ and $r = \theta_A(1)$. If $g^m \equiv 0 \pmod{n}$, then $\Gamma(A) \cong B(r, m)$.*

Proof. Let $\theta_A(x) = \sum_{i=0}^{r-1} x^{\alpha_i}$. Then by Theorem 1.3, each vertex in $\Gamma(A)$ can be uniquely represented as $\sum_{j=0}^{m-1} \alpha_{i_j} g^j$, $\alpha_{i_j} \in \{\alpha_0, \alpha_1, \ldots, \alpha_{r-1}\}$, $0 \leqslant j \leqslant m-1$. Since $g^m \equiv 0 \pmod{n}$, we have

$$\begin{aligned}&\left(\alpha_{i_0} + \alpha_{i_1} g + \cdots + \alpha_{i_{m-1}} g^{m-1}\right) g + \alpha_t \\ &\quad = \alpha_t + \alpha_{i_0} g + \alpha_{i_1} g^2 + \cdots + \alpha_{i_{m-1}} g^m \\ &\quad = \alpha_t + \alpha_{i_0} g + \alpha_{i_1} g^2 + \cdots + \alpha_{i_{m-2}} g^{m-1}\end{aligned}$$

for any $\alpha_t, \alpha_{i_j} \in \{\alpha_0, \alpha_1, \ldots, \alpha_{r-1}\}$, $j = 0, 1, \ldots, m-1$. Note that the adjacency rule in $\Gamma(A)$ is given by $u \to ug + \alpha$, $u \in V(\Gamma(A))$, $\alpha \in \{\alpha_0, \alpha_1, \ldots, \alpha_{r-1}\}$. Thus it is readily seen that the mapping φ: $V(\Gamma(A)) \to V(B(r, m))$ defined by

$$\varphi\left(\alpha_{i_0} g + \alpha_{i_1} g^2 + \cdots + \alpha_{i_{m-1}} g^{m-1}\right) = (i_{m-1}, i_{m-2}, \ldots, i_0),$$

$i_0, i_1, \ldots, i_{m-1} \in \{0, 1, \ldots, r-1\}$, induces an isomorphism from $\Gamma(A)$ to $B(r, m)$. □

Note that $g^m \equiv 0 \pmod{n}$ holds for any g-circulant in $P_{c,1,m}$. Therefore we have (see also [34]):

Corollary 6.1. *Any two matrices in $P_{c,1,m}$ are isomorphic.*

Let us turn to the presentation of our first main result in this section. It characterizes a special family of the well-known De Bruijn digraphs. (The reader can refer to [35] for a characterization of general De Bruijn digraphs.)

Theorem 6.1. *Suppose that $\operatorname{ord}_p(n) = m$ holds for every prime factor of n. Then any (0, 1) g-circulant solution A to $A^m = J_n$ is permutation similar to the adjacency matrix of $B(r, m)$.*

Proof. Since Theorem 3.1 implies in this case that $g^m \equiv 0 \pmod{n}$, the assertion follows from Lemma 6.1. □

We next turn our attention to the study of the isomorphism relations among the members of a class $P_{c,k,m}$ for any given c, k, m. In view of Corollary 6.1, we restrict our attention to $k \geqslant 2$.

Lemma 6.2. *Let A be a $(0, 1)$ g-circulant solution to $A^2 = J$ and $\theta_A(x) = \sum_{i=1}^{r} x^{a_i}$. Then $\Gamma(A)$ contains exactly r vertices, each of which has a loop attachment. Furthermore, the out-neighbor sets of these r vertices constitute a partition of $V(\Gamma(A))$.*

Proof. Let A be a g-circulant and $c = (g, n)$. Then by Theorem 3.1, any prime factor of n divides c. It follows that $(1 - g, n) = 1$. Thus we can choose $\rho \in \mathbb{Z}$ such that $\rho(1 - g) \equiv 1 \pmod{n}$. Let $\theta_A(x) = \sum_{i=1}^{r} x^{a_i}$. Observe that in $\Gamma(A)$, each vertex i is joined to $ig + a_j$, $1 \leqslant j \leqslant r$. So, it is not difficult to check that $\Gamma(A)$ contains exactly r loops $(\rho a_i, \rho a_i g + a_i)$, $i = 1, 2, \ldots, r$. Moreover, by Theorem 1.1, $\theta_A(x)\theta_A(x^g) \equiv T_n(x) \pmod{x^n - 1}$. Since $(g, n) = (\rho g, n)$, we see from Theorem 1.2 that $\theta_A(x)\theta_A(x^{\rho g}) \equiv T_n(x) \pmod{x^n - 1}$. This implies that $(\rho a_i)g + a_j$, $1 \leqslant i, j \leqslant r$, are pairwise distinct. Consequently, $V(\Gamma(A)) = \bigcup_{i=1}^{r} N^{+}_{\Gamma(A)}(\rho a_i)$, completing the proof. □

Remark. It can be easily obtained via eigenvalue argument that for any matrix A satisfying $A^2 = J_{r^2}$ it holds $Tr(A) = r$, from which the first claim of Lemma 6.2 also follows. But in order to get the second claim, the g-circulant condition cannot be removed, as we will illustrate it immediately. Let A_0 be the matrix displayed below:

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0
\end{bmatrix}.$$

It is verified that $A_0^2 = J$. Note that 0, 5, 10, 14 are the vertices with loop attachment in $\Gamma(A_0)$; but 12 is not in the union of the out-neighbor sets of these four vertices. As a by-product of Lemma 6.2, we know that A_0 is not permutation similar to any g-circulant.

Theorem 6.2. *All matrices in $P_{2,2,2}$ are isomorphic to each other.*

Proof. We will carry out computations in $\mathbb{Z}_{16}$ in most places without further assertion.

Let A be a g-circulant in $P_{2,2,2}$. Then A has order 16, constant line sum 4, and shifting parameter $g \equiv 2 \pmod 4$. Note that

$$g^2 = 4. \tag{25}$$

Let $\theta_A(x) = x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4}$ be the Hall polynomial of A. In view of Theorem 4.1, we know that there are some p's taking values in $\{0, 1\}$ such that

$$\begin{aligned}\{a_1, a_2, a_3, a_4\} = \{&2p_0 + 8p_{0,0}, 2p_0 + 8p_{0,1} + 4, 2p_1 + 8p_{1,0} + 1,\\ &2p_1 + 8p_{1,1} + 5\}.\end{aligned}$$

Hence, by rewriting the indices of a_i's if necessary, we may assume that

$$a_3 = a_1 + 4, \quad a_4 = a_2 + 4, \quad \text{and} \quad a_1 - a_2 \equiv 1 \pmod 4. \tag{26}$$

(Note that it is meaningful to write $a_1 - a_2 \equiv 1 \pmod 4$ in $\mathbb{Z}_{16}$ since 4 is a divisor of 16.) Consequently, by letting τ be the permutation $(13)(24)$ acting on $\{1, 2, 3, 4\}$, we have

$$4(a_i - a_j) = \begin{cases} 4 & \text{if } (i, j) \in \{1, 3\} \times \{2, 4\},\\ -4 & \text{if } (i, j) \in \{2, 4\} \times \{1, 3\},\end{cases} \tag{27}$$

$$g(a_j - a_{\tau(j)}) = 8, \tag{28}$$

$$(1 - g)(a_{\tau(k)} - a_k) = \begin{cases} 4 & \text{if } k \in \{3, 4\},\\ -4 & \text{if } k \in \{1, 2\}.\end{cases} \tag{29}$$

Observe that $(1 - g)(g - 3) = 1$ and hence it is meaningful to refer to $(1 - g)^{-1}$ (which is just $g - 3$ in $\mathbb{Z}_{16}$) here. Now the proof of Lemma 6.2 shows that $\Gamma(A)$ contains four vertices, enumerated as $u_i = (1 - g)^{-1}a_i$, $1 \leqslant i \leqslant 4$, such that

$$V(\Gamma(A)) = \bigcup_{i=1}^{4} N^+_{\Gamma(A)}(u_i) = \bigcup_{i=1}^{4} \{u_i g + a_j : 1 \leqslant j \leqslant 4\}. \tag{30}$$

For $1 \leqslant i, j, k \leqslant 4$, let

$$\pi_{i,k}(j) = \begin{cases} \tau(j) & \text{if } i + j \equiv 1 \pmod 2 \text{ and } (i, k) \in \{1, 3\} \times \{2, 4\},\\ j & \text{otherwise.}\end{cases}$$

We now assert that

$$(u_i g + a_j)g + a_k = u_{\pi_{i,k}(j)}g + a_k \quad \text{if } i \equiv j \ (\text{mod } 2), \tag{31}$$

$$(u_i g + a_j)g + a_k = u_{\pi_{i,\tau(k)}(j)}g + a_{\tau(k)} \quad \text{if } i \not\equiv j \ (\text{mod } 2). \tag{32}$$

Clearly (30)–(32) will imply that $E(\Gamma(A)) = \{u_i g + a_j \to u_{\pi_{i,k}(j)}g + a_k : 1 \leqslant i, j, k \leqslant 4\}$. Therefore, the mapping φ: $u_i g + a_j \mapsto (i, j)$ induces an isomorphism from $\Gamma(A)$ to the specific digraph $G = (V, E)$, where $V = \{(i, j) : 1 \leqslant i, j \leqslant 4\}$ and $E = \{(i, j) \to (\pi_{i,k}(j), k) : 1 \leqslant i, j, k \leqslant 4\}$, and hence our result will follow.

The remaining part is devoted to the proof of (31) and (32).

First consider the case $i \equiv j$ (mod 2). To see that (31) holds, we first note that if $i \equiv j$ (mod 2), then $\pi_{i,k}(j) = j$ for any k. Using this and (25), we have

$$\begin{aligned}
&(u_i g + a_j)g + a_k \\
&\quad = \big(u_{\pi_{i,k}(j)}g + a_k\big) + \big((u_i g + a_j)g + a_k\big) - \big(u_{\pi_{i,k}(j)}g + a_k\big) \\
&\quad = \big(u_{\pi_{i,k}(j)}g + a_k\big) + \big(u_i g^2 + a_j g - u_j g\big) \\
&\quad = \big(u_{\pi_{i,k}(j)}g + a_k\big) + \big(4a_i(1-g)^{-1} + a_j g - a_j(1-g)^{-1}g\big).
\end{aligned} \tag{33}$$

We can also deduce from (25) and (26) that

$$\begin{aligned}
4a_i + a_j g(1-g) - a_j g &= 4a_i - a_j g^2 \\
&= 4a_i - 4a_j \\
&= 0.
\end{aligned}$$

Multiplying this relation by $(1-g)^{-1}$, we obtain $4a_i(1-g)^{-1} + a_j g - a_j(1-g)^{-1}$ $g = 0$. Thus by virtue of (33), we see that (31) holds.

As for the case $i \not\equiv j$ (mod 2), we will turn to prove an equivalent formulation of (32), that is,

$$4(a_i - a_j) + g(a_j - a_{\pi_{i,k}(j)}) + (1-g)(a_{\tau(k)} - a_k) = 0, \tag{34}$$

which is obtained from (32) by multiplying $1 - g$ and then using (25). To verify (34), we will consider four cases individually:

(i) i is odd, j is even, and $k \in \{3, 4\}$;
(ii) i is odd, j is even, and $k \in \{1, 2\}$;
(iii) i is even, j is odd, and $k \in \{3, 4\}$;
(iv) i is even, j is odd, and $k \in \{1, 2\}$.

Note that in cases (i) and (iv) we have $\pi_{i,k}(j) = \tau(j)$ while in cases (ii) and (iii) we have $\pi_{i,k}(j) = j$. Now using (27), we get that, in cases (i) and (ii), $4(a_i - a_j) = 4$, while in cases (iii) and (iv), $4(a_i - a_j) = -4$; using (28), we get that in cases (i) and (iv), $g(a_j - a_{\pi_{i,k}(j)}) = 8$ while in cases (ii) and (iii) $g(a_j - a_{\pi_{i,k}(j)}) = g(a_j - a_j) = 0$; using (29), we get that in cases (i) and (iii), $(1-g)(a_{\tau(k)} - a_k) = 4$ while in cases (ii) and (iv), $(1-g)(a_{\tau(k)} - a_k) = -4$. After these preparations, it is then a trivial matter to check that (34) holds for all the four cases. The proof of the theorem is completed. □

We are now concluding this section by showing that there are always two non-isomorphic members in $P_{c,k,m}$ for rest of the cases, that is, all the three integers c, k, m are greater than 1 and at least one of them is greater than 2. We now give some additional notation and terminology. A nonempty proper subset S of $\mathbb{Z}_n$ is called a *circular set*, if there are two elements (not necessarily distinct) $l(S), r(S) \in \mathbb{Z}_n$ such that $S = \{l(S), l(S)+1, \ldots, r(S)\}$. It is obvious that the pair $(l(S), r(S))$ is uniquely determined by the circular set S. We call $l(S)$ $(r(S))$ the *left* (*right*) *end* of S. For any (0, 1) matrix A of order n we define $X_A = \{j \pmod n) : A(0, j) = 1\}$, which is a subset of $\mathbb{Z}_n$. Observe that if A is a g-circulant, then $\mathbb{N}^+_{\Gamma(A)}(i) = ig + X_A$ for any vertex i of $\Gamma(A)$.

Theorem 6.3. *Let c, k, m be three integers no less than 2 and at least one of them is greater than 2. Then there exist two non-isomorphic members in $P_{c,k,m}$.*

Proof. Write $n = c^{km}$. Let A_1 be the c-circulant whose Hall polynomial is obtained by assigning 0 to each p in (16), that is, $X_{A_1} = \{\sum_{j=1}^{k} i_j c^{(j-1)m} : 0 \leqslant i_j \leqslant c-1,\ 1 \leqslant j \leqslant k\}$. We know from Theorem 4.1 that $A_1 \in P_{c,k,m}$. (In fact, it is not difficult to check that $\theta_{A_1}(x) = \Phi_{c,k,m}(x)$.)

We will show that the number of the common out-neighbors of any two vertices u and v in $\Gamma(A_1)$ is a multiple of c, that is, $|\mathbb{N}^+_{\Gamma(\mathrm{A}_1)}(u) \cap \mathbb{N}^+_{\Gamma(\mathrm{A}_1)}(v)| \equiv 0 \pmod c$.

Denote by T the set consisting of all the $(k-1)$-tuples $(i_2, i_3, \ldots, i_k)$, $0 \leqslant i_j \leqslant c-1$, $2 \leqslant j \leqslant k$. For each $(i_2, i_3, \ldots, i_k) \in T$, we write $U_{i_2,i_3,\ldots,i_k} = \{\sum_{j=1}^{k} i_j c^{(j-1)m} : 0 \leqslant i_1 \leqslant c-1\}$. Observe that each $U_{i_2,i_3,\ldots,i_k}$ is a circular set in $\mathbb{Z}_n$. Furthermore, by comparing the cardinalities, we see that X_{A_1} is the disjoint union of $U_{i_2,i_3,\ldots,i_k}$'s for $(i_2, i_3, \ldots, i_k) \in T$. Henceforth,

$$\begin{aligned}
&\left|\mathbb{N}^+_{\Gamma(A_1)}(u) \cap \mathbb{N}^+_{\Gamma(A_1)}(v)\right| \\
&\quad = \left|(uc + X_{A_1}) \cap (vc + X_{A_1})\right| \\
&\quad = \left|\left(\bigcup_{(i_2,i_3,\ldots,i_k)\in T} (uc + U_{i_2,i_3,\ldots,i_k})\right) \cap \left(\bigcup_{(i'_2,i'_3,\ldots,i'_k)\in T} (vc + U_{i'_2,i'_3,\ldots,i'_k})\right)\right| \\
&\quad = \left|\bigcup_{(i_2,i_3,\ldots,i_k)\in T} \ \bigcup_{(i'_2,i'_3,\ldots,i'_k)\in T} \Big((uc + U_{i_2,i_3,\ldots,i_k}) \cap (vc + U_{i'_2,i'_3,\ldots,i'_k})\Big)\right| \\
&\quad = \sum_{(i_2,i_3,\ldots,i_k)\in T} \ \sum_{(i'_2,i'_3,\ldots,i'_k)\in T} \left|(uc + U_{i_2,i_3,\ldots,i_k}) \cap (vc + U_{i'_2,i'_3,\ldots,i'_k})\right|. \qquad (35)
\end{aligned}$$

Notice that for any $(i_2, i_3, \dots, i_k) \in T$, $U_{i_2,i_3,\dots,i_k}$ is of cardinality c and has left end $\sum_{j=2}^{k} i_j c^{(j-1)m} \equiv 0 \pmod{c}$. So we conclude that for any two $(k-1)$-tuples $(i_2, i_3, \dots, i_k)$, $(i'_2, i'_3, \dots, i'_k)$, the two circular sets $uc + U_{i_2,i_3,\dots,i_k}$ and $vc + U_{i'_2,i'_3,\dots,i'_k}$ are either identical or disjoint. This then allows us to derive from (35) that

$$\left|\mathbb{N}^+_{\Gamma(A_1)}(u) \cap \mathbb{N}^+_{\Gamma(A_1)}(v)\right| \equiv 0 \pmod{c}. \tag{36}$$

We now take the c-circulant A_2 with $X_{A_2} = \left(X_{A_1} \backslash \{\alpha\}\right) \cup \{\beta\}$, where $\alpha = (c-1)\sum_{i=0}^{k-1} c^{im}$ and $\beta = (c-1)\sum_{i=0}^{k-1} c^{im} + c^{(k-1)m+1}$. Note that $\theta_{A_2}(x)$ is indeed a member of $\Omega_{c,k,m}$ which can be represented as in (16) with all but one p's equal to 0, and the exceptional case is

$$p_{\underbrace{c-1, c-1, \dots, c-1}_{k \text{ elements}}} = 1.$$

Clearly,

$$\begin{aligned} X_{A_2} \cap (c^m + X_{A_2}) &= (Z_1 \cup Z_2) \cap (Z_3 \cup Z_4) \\ &= (Z_1 \cap Z_3) \cup (Z_1 \cap Z_4) \cup (Z_2 \cap Z_3) \cup (Z_2 \cap Z_4), \end{aligned}$$

where $Z_1 = X_{A_1} \backslash \{\alpha\}$, $Z_2 = \{\beta\}$, $Z_3 = c^m + (X_{A_1} \backslash \{\alpha\})$, and $Z_4 = \{c^m + \beta\}$.

It immediately follows from $c, k, m \geqslant 2$ and $n = c^{km}$ that $Z_2 \cap Z_3 = Z_2 \cap Z_4 = \emptyset$.

In order to see that $Z_1 \cap Z_4 = \emptyset$, it is enough to prove the inequality

$$(c-1)\sum_{i=0}^{k-1} c^{im} + c^{(k-1)m+1} + c^m < c^{km}. \tag{37}$$

Surely, our assumption on c, k, and m namely $c, k, m \geqslant 2$ and at least one of them is greater than 2 is needed in our reasoning below. Let $x = (c^{m-1} - 1)(\sum_{i=0}^{k-2} c^{im+1})$ and $y = (c^{m-1} - 2)c^{(k-1)m+1}$. If $k > 2$, then $x > c^m$; while if one of c and m is greater than 2, then $c^{m-1} > 2$ and hence $y > c^m$. But x and y are both nonnegative quantities whatever the case is. So it follows $x + y > c^m$. Note that $(c-1)\sum_{i=0}^{k-1} c^{im}$ $+c^{(k-1)m+1} + x + y = c^{km} - 1$. Therefore, (37) comes from $x + y > c^m$, as desired.

By now, we have

$$\begin{aligned} \mathbb{N}^+_{\Gamma(A_2)}(0) \cap \mathbb{N}^+_{\Gamma(A_2)}(c^{m-1}) &= X_{A_2} \cap (c^m + X_{A_2}) \\ &= Z_1 \cap Z_3 \\ &= \left(X_{A_1} \backslash \{\alpha\}\right) \cap \left(c^m + \left(X_{A_1} \backslash \{\alpha\}\right)\right) \\ &= \left(X_{A_1} \cap \left(c^m + X_{A_1}\right)\right) \backslash \{\alpha\} \\ &= \left(\mathbb{N}^+_{\Gamma(A_1)}(0) \cap \mathbb{N}^+_{\Gamma(A_1)}(c^{m-1})\right) \backslash \{\alpha\}. \end{aligned}$$

This together with (36) implies that

$$\left|\mathbb{N}^{+}_{\Gamma(A_2)}(c^{m-1}) \cap \mathbb{N}^{+}_{\Gamma(A_2)}(0)\right| \equiv (c-1) \pmod{c}. \tag{38}$$

Comparing (38) with (36), we get that $\Gamma(A_1)$ and $\Gamma(A_2)$ are not isomorphic. Hence $A_1 \ncong A_2$. □

7. Open problems

Of course, the main challenge in this subject is to tackle Wang's conjecture. But our work above suggest some smaller problems.

First, is it always true that all k's appearing in Theorem 3.1 must take the same value? Second, even if all k's already have the same value, say just k, can we assert that $\Phi_{c,k,m}(x) \mid \theta(x)$? Note that Wang's conjecture means that these two problems both have affirmative answers.

The work in Section 3 relies heavily on the property of root sets of polynomials in F_n. But F_n is nothing but $\Omega'_{n,1,m}$. It seems interesting to see if anything worthwhile can be said about the root sets of polynomials in a general $\Omega'_{c,k,m}$ or $\Omega_{c,k,m}$. We remark that a key argument in the proof of Theorem 3.1 amounts to showing that

$$\left(\prod_{i=1}^{k-1} T_{p^{\alpha}}\left(x^{p^{\alpha(im-1)}}\right)\right), \prod_{i=0}^{m-2} \theta\left(x^{c^{i}}\right)) = 1,$$

where p is a prime and $\alpha = \operatorname{ord}_p(c)$, by using Lemma 2.7. Hence we would like to ask if it can occur

$$\left(\prod_{i=1}^{k-1} T_b\left(x^{b^{im-1}}\right), \prod_{i=0}^{m-2} \theta\left(x^{c^{i}}\right)\right) \neq 1$$

for some b, c, and $\theta(x)$, where $b \mid c$, $(b,\ b/c) = 1$ and $\theta(x) \in \Omega_{c,k,m}$.

The techniques in Sections 3 and 5 are rather different and they play separate role in the approach here. It may be a good idea to try to combine them to obtain further results. Particularly, by comparing those results in Sections 3 and 5, we pose the following question: if a (0, 1) polynomial $\theta(x)$ satisfies $\theta(1) = c^k u,\ (c, u) = 1$, $\Phi_{c,k,m}(x) \mid \theta(x)$, and $\prod_{i=0}^{m-1} \theta(x^{g^i}) \in F_n$, must it hold that $(c, g/c) = 1$?

We have discussed the isomorphism problem for those matrices in a fixed $P_{c,k,m}$. Let $A(c, k, m)$ be the c-circulant with Hall polynomial $\Phi_{c,k,m}(x)$ and order c^{km}. By computing the rank of $A(c, k, m)$, Wang and Wang [34] proved that two $A(c, k, m)$'s can be isomorphic only if they have the same parameters, i.e., they are the same matrix. It still remains an open problem whether there are two isomorphic matrices occurring in different $P_{c,k,m}$'s.

Finally, let us present a conjecture which may be somewhat "bigger" than the conjecture of Wang. Let $n = \prod_{i=1}^{km} n_i$, where $n_i, i = 1, \ldots, km$, are natural numbers. Let $n_0 = 1$. For $i = 0, \ldots, m-1$, define a $(0, 1)$ polynomial $f_i(x)$ to be $\prod_{j=0}^{k-1} (x^{p_{i+1+jm}} - 1)/(x^{p_{i+jm}} - 1)$, where $p_s = \prod_{i=0}^{s} n_i$ for $s = 0, \ldots, km$. Clearly, $(x^n - 1)/(x - 1) = \prod_{i=0}^{m-1} f_i(x)$, which will be called a standard factorization of $(x^n - 1)/(x - 1)$ corresponding to the factorization $n = \prod_{i=1}^{km} n_i$. Our conjecture is: all factorizations of $(x^n - 1)/(x - 1)$ into a product of $(0, 1)$ polynomials must be a standard factorization. Restricting to the case that we factorize $(x^n - 1)/(x - 1)$ into a product of two polynomials, this conjecture has long been known to be true, according to a famous result of De Bruijn [2]. For its connection with the topic we have addressed here please note that for any c, k, m, $\prod_{i=0}^{m-1} \Phi_{c,k,m}(x^{c^i})$ all are standard factorizations of $(x^n - 1)/(x - 1)$ provided that $n = c^{km}$, while Wang's conjecture means that these factorizations are "generators" of all solutions to Eq. (1). In the study of perfect graph, there is a problem on finding two subsets A, B of $\mathbb{Z}_n$ such that $|A + B| = |A||B| = n - 1$ [1,5,10]. Conjecture 2.1 in [1] can be interpreted as any such subset pair A, B of $\mathbb{Z}_n$ must correspond to a so-called "De Bruijn near-factorization" of $\mathbb{Z}_n$. We remark that any "De Bruijn near-factorization" of $\mathbb{Z}_n$ corresponds instead to a standard factorization of $(x^{n-1} - 1)/(x - 1)$ into two $(0, 1)$ polynomials (see [1,2,10] for details). As is clear now, the two conjectures on additive property of $\mathbb{Z}_n$, namely, Wang's conjecture and the conjecture in [1] as described above, both have close connection with the concept of standard factorization. Perhaps it may be true that the two conjectures on $\mathbb{Z}_n$ can be deduced from our conjecture and it will be interesting to see if such a deduction can really be given.

References

[1] G. Bascó, E. Boros, V. Gurvich, F. Maffray, M. Preissmann, On minimal imperfect graphs with circular symmetry, J. Graph Theory 29 (1998) 209–225.

[2] N.G. de Bruijn, On number systems, Nieuw Arch. Wisk. 3 (1956) 15–17.

[3] C.Y. Chao, T. Wang, On the matrix equation $A^2 = J$, J. Math. Res. Exposition 2 (1987) 207–215.

[4] E.M. Coven, A. Meyerowitz, Tiling the integers with translates of one finite set, J. Algebra 212 (1999) 161–174.

[5] V. Chvátal, R.L. Graham, A.F. Perold, S.H. Whitesides, Combinatorial designs related to the perfect graph conjecture, Discrete. Math 26 (1979) 83–92.

[6] A.M. Duval, A directed graph version of strongly regular graphs, J. Combin. Theory A 47 (1988) 71–100.

[7] M.A. Fiol, I. Alegre, J.L.A. Yebra, J. Fabrega, Digraphs with walks of equal length between vertices, in: Y. Alavi et al. (Eds.), Graph Theory with Applications to Algorithms and Computer Science, Wiley, New York, 1985, pp. 313–322.

[8] M.A. Fiol, J. Gimbert, J. Gómez, Y. Wu, On Moore bipartite digraphs (submitted).

[9] D. Goldfeld, T. Etzion, UPP graphs and UMFA network—architecture for parallel systems, IEEE Trans. Comput. 41 (11) (1992) 1479–1483.

[10] C. Grinstead, On circular critical graphs, Discrete. Math. 51 (1984) 11–24.

[11] A.J. Hoffman, Research problems 2–11, J. Combin. Theory 2 (1967) 393.

[12] A.J. Hoffman, M.H. McAndrew, The polynomial of a directed graph, Proc. Amer. Math. Soc. 16 (1965) 303–309.

[13] T.W. Hungerford, Algebra, Springer, Berlin, 1980.

[14] F. King, K. Wang, On the g-circulant solutions to the matrix equation $A^m = \lambda J$, J. Combin. Theory Ser. A 38 (1985) 182–186.

[15] M. Klin, A. Munemasa, M. Muzychuk, P.-H. Zieschang, Directed strongly regular graphs via coherent (cellular) algebras, preprint.

[16] D.E. Knuth, Notes on central groupoids, J. Combin. Theory 8 (1970) 376–390.

[17] C.W.H. Lam, On some solutions of $A^k = dI + \lambda J$, J. Combin. Theory Ser. A 23 (1977) 140–147.

[18] C.W.H. Lam, A generalization of cyclic difference sets, J. Combin. Theory Ser. A 19 (1975) 51–65.

[19] C.W.H. Lam, A generalization of cyclic difference sets II, J. Combin. Theory Ser. A 19 (1975) 177–191.

[20] H. Lu, On the matrix equation $A^m = \lambda J$, Acta Math. Appl. Sinica 14 (2) (1991) 155–163 (in Chinese).

[21] S.L. Ma, W.C. Waterhouse, The g-circulant solutions of $A^m = \lambda J$, Linear Algebra Appl. 85 (1987) 211–220.

[22] M. Malyshev, V.E. Tarakanov, Generalized De Bruijn graphs, Math. Notes 62 (4) (1997) 449–456.

[23] N.S. Mendelsohn, Directed graphs with the unique path property, in: P. Erdős, A. Renyi, V.T. Sos (Eds.), Combinatorial Theory and its Applications, North-Holland, Amsterdam, 1970, pp. 783–799.

[24] N.S. Mendelsohn, An application of matrix theory to a problem in universal algebra, Linear Algebra Appl. 1 (1968) 471–478.

[25] H.J. Ryser, A generalization of the matrix equation $A^m = J$, Linear Algebra Appl. 3 (1970) 451–460.

[26] L.E. Shader, On the existence of finite central groupoids of all possible ranks I, J. Combin. Theory A 16 (1974) 221–229.

[27] M.A. Sridhar, C.S. Raghavendra, Uniform minimal full-access networks, J. Parallel Distribut. Comput. 5 (1988) 383–403.

[28] M.A. Sridhar, C.S. Raghavendra, Fault-tolerant networks based on De Bruijn graph, IEEE Trans. Comput. 40 (10) (1991) 1167–1174.

[29] M.A. Sridhar, C.S. Raghavendra, Minimal full-access networks: enumeration and characterization, IEEE Trans. Comput. 9 (1990) 347–356.

[30] J. Wang, The number and construction of solutions of some congruence and their combinatorial applications, PhD Thesis, Dalian University of Technology, 1990 (in Chinese).

[31] J. Wang, Private communication.

[32] K. Wang, On the matrix equation $A^m = \lambda J$, J. Combin. Theory Ser. A 29 (1980) 134–141.

[33] K. Wang, On the g-circulant solutions to the matrix equation $A^m = \lambda J$, J. Combin. Theory Ser. A 33 (1982) 287–296.

[34] T. Wang, J. Wang, On some solutions to the matrix equation $\mathrm{A}^m = J$, J. Dalian Univ. Tech. 10 (1990) 621–624 (in Chinese).

[35] Y. Wu, R. Jia, Q. Li, A characterization of De Bruijn digraphs (submitted).

In the proof-reading process, we wanted to improve the presentation of Lemma 2.3. Unfortunately, when writing email to inform the publisher of our modification, I wrote mistakenly Lemma 2.3 as Lemma 2.2. Thus, in the published version of this paper, Lemma 2.3 appears just in the same way as in the proof sent to us and Lemma 2.2 is substituted by the updated version of Lemma 2.3 as described in our email to the publisher. Please note that these two lemmas should read as follows.

Lemma 2.2

$$T_r(x^s) = \prod_{\substack{t|rs \\ t\nmid s}} \phi_t(x).$$

Hence all roots of $T_r(x^s) = 0$ are simple roots and $Root(T_r(x^s)) = \{\xi\colon \xi$ is a root of unity whose order t satisfies $t \mid rs$ and $t \nmid s\}$.

Proof: It follows immediately from the fact that $T_r(x^s)$ is just $(1 - x^{rs})/(1 - x^s)$ and it holds $1 - x^h = \prod\limits_{t|h} \phi_t(x)$ for $h = rs$ and s. □

Lemma 2.3 Let $f(x) \in Z^*[x]$ and $c, k, m \in \mathbf{N}$. If $\Phi_{c,k,m}(x) \mid f(x)$ in $C[x]$, then $f(1) \geq c^k$. If $f(1) = c^k$ then $f(x)$ must be a $(0, 1)$ polynomial, namely, a polynomial each of whose coefficients is either 0 or 1, and $h(x) \equiv T_n(x)$ $(mod\ x^n - 1)$, where $n = c^{km}$ and $h(x) = \prod_{i=0}^{m-1} f(x^{c^i})$.

Proof: Recall that $\Phi_{c,k,m}(x) = \prod_{i=0}^{k-1} T_c(x^{c^{im}})$. It is easily seen that $\prod_{i=0}^{m-1} \Phi_{c,k,m}(x^{c^i}) = T_n(x)$. Hence by hypothesis, there is $g(x)$ such that $h(x) = T_n(x)g(x)$. Since $T_n(x), h(x) \in Z[x]$ and $T_n(x)$ is monic, we then get $g(x) \in Z[x]$. By setting $x = 1$, we immediately obtain $f(1)^m = h(1) \geq T_n(1) = c^{km}$ and hence $f(1) \geq c^k$. If $f(1) = c^k$, then $h(1) = n$. Thus we can deduce from Corollary 2.1 that $h(x)$ is a $(0, 1)$ polynomial and $h(x) \equiv T_n(x)$ $(mod\ x^n - 1)$. Because $h(x) = \prod_{i=0}^{m-1} f(x^{c^i})$ and $f(x) \in Z^*[x]$, we see that $f(x)$ is a $(0, 1)$ polynomial too. □