ELSEVIER Linear Algebra and its Applications 295 (1999) 249–260

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

On the matrix equation $A^k = J - I$

Yaokun Wu [1], Qiao Li *, Xuyan Huang [2]

Department of Applied Mathematics, Shanghai Jiao Tong University, 1954 Huashan Road, Shanghai 200030, People's Republic of China

Received 6 July 1998; accepted 29 December 1998

Submitted by R.A. Brualdi

Abstract

We concern ourselves with the problem of solving the $(0, 1)$ matrix equation $A^k = J - I$ in this paper, where J is the matrix of all one's, I the identity matrix and A an unknown $(0, 1)$ matrix. In particular, our effort brings about a complete solution of $A^k = J_{2^k+1} - I_{2^k+1}$. This generalizes a theorem of Lam and Van Lint. In the course of our solution we provide a local characterization of the webs, i.e., the powers of the cycles. Our results mainly rely on the analysis of the intersection pattern of a collection of some specific sets, namely, the row sets of a matrix; some results on partitionable graphs are also introduced to tackle this problem. Our work suggests an approach to investigate $A^k = J - I$ by studying a number-theoretical question and a conjecture of Ravindra on partitionable graphs. Several open problems are also presented. © 1999 Elsevier Science Inc. All rights reserved.

AMS classification: 05C50; 15A24

Keywords: Matrix equation; Circulant; Row sets; Partitionable graph; Web

1. Introduction

We always use the notation J for the matrix with every entry equal to 1 and I for the identity matrix. Let e_i be the $1 \times n$ matrix with 1 in the $(i + 1)$th leftmost

* Corresponding author. E-mail: mathpo@mail.sjtu.edu.cn

[1] E-mail: yaokunwu@public2.sta.net.cn

[2] E-mail: branchxi@263.net

PII: S 0 0 2 4 - 3 7 9 5 (9 9) 0 0 0 2 1 - X

position and 0's elsewhere. The $n \times n$ permutation matrix N is the unique one satisfying $e_{n-1}N = e_0$ and $e_iN = e_{i+1}$ for $i = 0, 1, \dots, n-2$. The matrix Q_p will denote the one which satisfies $e_0Q_p = e_0$ and $NQ_p = Q_pN^p$ for any $p \in Z_n$; that is, Q_p is the *p-circulant* [14] with first row e_0. Sometimes we also use a subscript to indicate the size of a matrix.

The $(0,1)$ matrix equation $J - I = XY$ for two unknown matrices X and Y has an intimate connection with many discrete mathematics problems [1–3, 5–12,15–19,21–24]. Our paper is on one of its special cases, namely, the equation

$$A^k = J_n - I_n, \tag{1.1}$$

where k is a positive integer and A is an unknown $(0,1)$ matrix of order n. It is known that (1.1) is solvable if and only if k is odd and there is a nonnegative integer d such that $n = d^k + 1$ [18,21]. Each solution A must have constant line sums d. The case $d = 1$ is trivial. So in the rest of this paper we agree that k is odd and n is of the form $d^k + 1$ for some integer d greater than one.

As usual, we look on two solutions to (1.1) which are permutation similar as the same. We have shown that the solutions A to (1.1) are not unique in this sense in general [23]. On the other hand, some uniqueness results can be established. For example, we have proved that the spectrum of A and the numbers of short elementary cycles of the digraph of A are uniquely determined by (1.1) [24].

We write a number a in boldface always to mean its corresponding element in Z_n, that is, the residue class $a(\text{mod } n)$, except in the proof of Theorem 4.2. Let $f(x) = x + x^2 + \cdots + x^d$ and $M = Q_{-\mathbf{d}}f(N)$. It is well known that the $(-d)$-circulant M is a solution of (1.1) [8,18,21]. In Theorem 2.1, we prove that if $A^k = J - I$ and $A = P^{\mathrm{T}}M$ for some permutation matrix P, then for some q, the matrix A must be of the form $Q_{\mathbf{s}}f(N)N^q$, where $d|s|d^{k-1}$ and $\mathbf{s^k} = \mathbf{1}$. We remark here that we have found all the distinct solutions A to (1.1) up to permutation similarity under the assumption that A is permutation similar to a matrix of the form $Q_{(-\mathbf{d})^t}f(N)N^q$ for some t and q [23].

Section 3 contains two immediate corollaries of Theorem 2.1. They are obtained by using a result developed in [22,23].

Finally, we introduce in Section 4 a partitionable graph approach to show how it can be guaranteed that $A = P^{\mathrm{T}}M$ holds for some permutation matrix P. This in turn leads to a complete solution of (1.1) in the case of $d = 2$, which is a generalization of a theorem of Lam and Van Lint [18].

2. Relationship among the row sets of A^k, A^{k-1}, and A

We will use the symbol $a\downarrow$ for the least nonnegative integer x such that $\mathbf{a} = \mathbf{x}$ for any integer a. For any two sets C and D, let $C \setminus D = \{x | x \in C,$

$x \notin D\}$, $C \Delta D = (C \setminus D) \cup (D \setminus C)$, $C + D = \{x + y \,|\, x \in C,\ y \in D\}$, $C - D = \{x - y \,|\, x \in C,\ y \in D\}$.

For any matrix B of order n, the set $\{\boldsymbol{j} \,|\, e_{i\downarrow} B e_{j\downarrow}^{\mathrm{T}} > 0\}$, which is a subset of Z_n, is denoted by $B(i)$. The $B(i)$'s form a collection of subsets of Z_n, called the set of row sets of B. Clearly (1.1) displays the row sets of A^k. If we also know that the set of row sets of A is of some specific form, then the following theorem, Theorem 2.1, will help us to understand the structure of A by giving a picture of the row sets of A. In the proof of Theorem 2.1, we shall first consider the row sets of A^{k-1} rather than examining those of A directly.

Theorem 2.1. *If $A^k = J - I$, and $A = P^{\mathrm{T}} M$ for some permutation matrix P, then there is an integer q such that $A = Q_s f(N) N^q$ for some s such that $\boldsymbol{s^k} = \mathbf{1}$ and $d | s | d^{k-1}$.*

Proof. Suppose we already know that the solution A to (1.1) is of the form $Q_s f(N) N^q$ for some s and q. Since A^k is a nonsingular s^k-circulant, while $J - I$ is a 1-circulant, we conclude that $\boldsymbol{s^k} = \mathbf{1}$ by the same argument that appeared in [22]. So it only remains to show $A = Q_s f(N) N^q$ for some q and s such that $d | s$ and $s | d^{k-1}$.

In what follows, A^{k-1} will be abbreviated to X and the only element in $P(i)$ designated as P_i.

From the computation in [21], we know that $M(i) = \{-\boldsymbol{di} + \boldsymbol{t} \,|\, t = 1, 2, \ldots, d\}$ and $M^{k-1}(i) = \{\boldsymbol{d^{k-1} i} - \boldsymbol{t} \,|\, t = 0, 1, \ldots,\ d^{k-1} - 1\}$. Moreover, as an easy consequence of $A = P^{\mathrm{T}} M$, $A^k = J - I = M^k$, and $\det(J - I) \neq 0$, we find that $A^{k-1} = M^{k-1} P$. Thus $X(i) = \{P_{d^{k-1} i - t} \,|\, t = 0, 1, \ldots, d^{k-1} - 1\}$ follows. Because $d^k = n - 1$, we have

$$X(i) \setminus X(i + d) = P(d^{k-1} i), \tag{2.1}$$

$$X(i + d) \setminus X(i) = P(d^{k-1} i - d^{k-1}), \tag{2.2}$$

$$X(i) \cap X(j) = \emptyset \quad \text{if } 0 < |i - j| < d. \tag{2.3}$$

Define $[\boldsymbol{a}, \boldsymbol{b}]$ to be the subset $\{\boldsymbol{a}, \boldsymbol{a} + \mathbf{1}, \ldots, \boldsymbol{a} + (\boldsymbol{b} - \boldsymbol{a}) \downarrow\}$ of Z_n. We call it a circular r-set of Z_n, where $r = (b - a) \downarrow + 1$ is the size of $[\boldsymbol{a}, \boldsymbol{b}]$. Obviously $r \leqslant n$. If $r \neq n$, we say that $\boldsymbol{a}$ and $\boldsymbol{a} + \boldsymbol{r} - \mathbf{1}$ are the endpoints of $[\boldsymbol{a},\ \boldsymbol{a} + \boldsymbol{r} - \mathbf{1}]$. A segment of a subset T of Z_n is a maximal circular subset of T under inclusion.

Notice that every $M(i)$ is a circular d-set, and A is obtained from M by permuting the rows. Hence we certainly have every $A(i)$ is a circular d-set too.

$X(i)$ can be uniquely expressed as the disjoint union of its segments, say $X(i) = \bigcup_{j=1}^{t_i} X_j(i)$ for some t_i. Without loss of generality, assume $P_{d^{k-1} i} \in X_1(i)$. We refer to $Y(i)$ as the segment of $X(i)$ which contains $P_{d^{k-1} i - (d^{k-1} - 1)}$.

Since $X = A^{k-2}A$, each row of X is a sum of rows of A. Because A and X are $(0,1)$ matrices and the $A(i)$'s are circular d-sets, it follows that

$$d \,|\, |X_j(i)|. \tag{2.4}$$

Now we consider two cases.

Case A: $t_0 = t_1 = \cdots = t_{n-1} = 1$.

Since $X(i)\Delta X(i+d)$, the symmetric difference of two circular d^{k-1}-sets, is just $\{P_{d^{k-1}i}, P_{d^{k-1}(i-1)}\}$, we get $P_{d^{k-1}i} - P_{d^{k-1}(i-1)} = \pm \boldsymbol{d^{k-1}}$. We assert that $\boldsymbol{f_i} = P_{d^{k-1}i} - P_{d^{k-1}(i-1)}$ must be of the same value for all i. Otherwise, we should have some j such that $\boldsymbol{f}_j \neq \boldsymbol{f}_{j+1}$ and so $\boldsymbol{f_j} = -\boldsymbol{f_{j+1}}$. It follows $P_{d^{k-1}(j-1)} = P_{d^{k-1}(j+1)}$. But $0 < 2d^{k-1} \leqslant d^k < n$ implies $\boldsymbol{d^{k-1}(j-1)} \neq \boldsymbol{d^{k-1}(j+1)}$, which contradicts the fact that P is a permutation matrix. Therefore our assertion is verified. This means $\{\, P_i - P_{i-d^{k-1}} \,|\, i = 1, \ldots, n\} = \{P_{d^{k-1}i} - P_{d^{k-1}(i-1)} \,|\, i = 1, \ldots, n\} = \{-\boldsymbol{d^{k-1}}\}$ or $\{\boldsymbol{d^{k-1}}\}$. Hence $P = Q_{-1}N^t$ or Q_1N^t for some t. So we achieve that $A = P^{\mathrm{T}}Q_{-d}f(N) = Q_{\pm 1}Q_{-d}f(N)N^{\pm td} = Q_{\mp d}f(N)N^{\pm td}$. It is not difficult to establish the theorem by now.

Case B: There is some $t_s > 1$.

We first observe that it is true for all i that

$$P_{d^{k-1}i} \text{ is an endpoint of both } X_1(i) \text{ and } Y(i+d+1). \tag{2.5}$$

The reason is that $X_1(i) \cap Y(i+d+1)$, the intersection of two circular sets, is just $P(d^{k-1}i)$.

Here we should distinguish two subcases again.

Subcase B.1: $X_1(s) = [\boldsymbol{a}, P_{sd^{k-1}}]$, $Y(s+d+1) = [P_{sd^{k-1}}, \boldsymbol{b}]$.

Because $X_1(s)$ is a segment of $X(s)$ and $|X_1(s)| < n$, we obtain $\boldsymbol{a}\boldsymbol{-1} \notin X(s)$. However, the circular set $X_1(s) \setminus P(sd^{k-1})$ must be included in a segment of $X(s+d)$, say Y, by (2.1). Furthermore, (2.3) shows $Y \cap Y(s+d+1) = \emptyset$. But (2.4) says $|Y| \equiv 0 \pmod d$ while $|X_1(s) \setminus P(sd^{k-1})| \equiv -1 \not\equiv 0 \pmod d$. So (2.2) implies that $\boldsymbol{a}\boldsymbol{-1} = P_{(s-1)d^{k-1}} \in Y$. Now the definition of $Y(s+d)$ tells us $Y(s+d) = Y$ and hence it follows $Y(s+d) + \{\boldsymbol{1}\} = X_1(s) = [P_{(s-1)d^{k-1}} + \boldsymbol{1}, P_{sd^{k-1}}]$ by noting (2.5) in addition. Note at this point, that we can deduce from (2.3) and (2.5) that $X_1(s-1) = [\boldsymbol{a}', P_{(s-1)d^{k-1}}]$ and $Y(s+d) = [P_{(s-1)d^{k-1}}, \boldsymbol{b}']$ for some $\boldsymbol{a}'$ and $\boldsymbol{b}' = P_{sd^{k-1}} - \boldsymbol{1}$ as well. Thus the same argument applies to give $X_1(s-1) = Y(s-1+d) + \{\boldsymbol{1}\} = [P_{(s-2)d^{k-1}} + \boldsymbol{1}, P_{(s-1)d^{k-1}}]$. Continuing like this, we get

$$X_1(i) = Y(i+d) + \{\boldsymbol{1}\} = [P_{d^{k-1}(i-1)} + \boldsymbol{1}, P_{d^{k-1}i}] \tag{2.6}$$

holds for all i. Now (2.1), (2.2) and (2.6) together imply that

$$\begin{aligned}&\text{any segment of } X(i) \text{ other than } X_1(i) \text{ is also a segment}\\ &\text{of } X(i+d), \text{ and any segment of } X(i+d) \text{ other than } Y(i+d)\\ &\text{is a segment of } X(i) \text{ conversely.}\end{aligned} \tag{2.7}$$

So $t_i = t_{i+d}$ for all i. This means all the $X(i)$'s must have the same number of segments, say $t = t_s > 1$.

We further require that (2.6) still holds for each i, that is, $\boldsymbol{a_1(i)} = P_{d^{k-1}(i-1)} + \boldsymbol{1}$ and $\boldsymbol{b_1(i)} = P_{d^{k-1}i}$. We remark that this labeling does not affect the validity of any of our claims before.

Clearly (2.3) and (2.6) together imply that $\bigcup_{j=1}^{d-1} X_1(i+j) = [\boldsymbol{b_1(i)+1, a_1(i+d)-1}]$ lies in $[\boldsymbol{b_1(i)+1, a_2(i)-1}]$. Hence $\boldsymbol{a_1(i+d)} \in [\boldsymbol{b_1(i)+2, a_2(i)}]$. However, by looking at the distribution of the segments of $X(i)$, we see that $\boldsymbol{a_1(i)-1}$, the only element in $X(i+d)\setminus X(i)$, is not in $[\boldsymbol{b_1(i)+1, a_2(i)-1}]$. Thus, it follows from $X(i) \cap [\boldsymbol{b_1(i)+1, a_2(i)-1}] = \emptyset$ that $\boldsymbol{a_1(i+d)} \notin [\boldsymbol{b_1(i)+1, a_2(i)-1}]$ and henceforth $\boldsymbol{a_1(i+d)} = \boldsymbol{a_2(i)}$. So we arrive at $X_1(i+d) = X_2(i)$ by using (2.7). Noting our labeling rule in addition, we find that (2.6) and (2.7) imply now the relations below for all i:

$$X_j(i+d) = X_{j+1}(i) \quad \text{if } j = 1, 2, \ldots, t-1, \tag{2.8}$$

$$X_t(i+d) = Y(i+d) = X_1(i) - \{\boldsymbol{1}\}. \tag{2.9}$$

Combining (2.8) and (2.9), we obtain

$$X_1(i+td) = X_2(i+(t-1)d) = \cdots = X_t(i+d) = X_1(i) - \{\boldsymbol{1}\}. \tag{2.10}$$

It follows

$$\{X_1(tdj) \mid j = 1, 2, \ldots, n\} = \{X_1(0) - \{\boldsymbol{j}\} \mid j = 1, 2, \ldots, n\}. \tag{2.11}$$

Since the cardinality of the set on the right-hand side of (2.11) is n, we have

$$\{X_1(0) - \{\boldsymbol{j}\} \mid j = 1, 2, \ldots, n\} = \{X_1(j) \mid j = 1, 2, \ldots, n\}.$$

Therefore, all the numbers $|X_1(j)|$'s are equal. We denote this common value by r.

Let $T(q) = \bigcup_{j=1}^{d} X_1(qd+j)$. Then (2.3) and (2.6) demonstrate that $|T(q)| = dr$ and $T(q) = [\boldsymbol{a_1(qd+1), b_1(qd+d)}]$. Let us carry out the following calculations:

$$\boldsymbol{a_1(qd+1)} = \boldsymbol{a_{1+q}(1)} \quad \text{for } 0 \leqslant q \leqslant t-1 \qquad \text{(by 2.8)},$$

$$\begin{aligned} \boldsymbol{b_1(qd+d)} &= \boldsymbol{a_1(qd+d+1)-1} \qquad \text{(by 2.6)} \\ &= \boldsymbol{a_{q+2}(1)-1} \quad \text{for } 0 \leqslant q \leqslant t-2 \qquad \text{(by 2.8)}, \end{aligned}$$

$$\begin{aligned} \boldsymbol{b_1((t-1)d+d)} &= \boldsymbol{a_1(td+1)-1} \qquad \text{(by 2.6)} \\ &= \boldsymbol{a_1(1)-2} \qquad \text{(by 2.10)}. \end{aligned}$$

They show us that $T(q) = [\boldsymbol{a_{1+q}(1)},\ \boldsymbol{a_{2+q}(1)-1}]$ for $q = 0,\ 1, \ldots, t-2$, and $T(t-1) = [\boldsymbol{a_t(1)},\ \boldsymbol{a_1(1)-2}]$. But it is assumed that $a_1(1) < a_2(1) < \cdots$

$< a_t(1) < a_1(1) + n$. So we obtain $[\boldsymbol{a_1}(\mathbf{1}),\ \boldsymbol{a_1}(\mathbf{1}) - \mathbf{2}]$ is the disjoint union of $T(q)$ for $q = 0, 1, \ldots, t-1$. Therefore, $d^k = n - 1 = tdr$. It turns out that

$$r \,|\, d^{k-1}. \tag{2.12}$$

To finish the proof, we conclude from (2.6) that $P_{j+d^{k-1}} - P_j = \boldsymbol{r}$ holds for all j. Consequently P is of the form $Q_{r/d^{k-1}}N^v$ for some r and v. (We remark that the r/d^{k-1} appearing here should be viewed as a number in Z_n and is really meaningful since $\gcd(n, d^{k-1}) = 1$.) Hence $A = P^{\mathrm{T}}M = Q_{-d^k/r}f(N)N^q$ for some q. Noting (2.4) and (2.12), the theorem is established in this subcase by letting $s = -d^k/r$.

Subcase B.2: $X_1(s) = [P_{sd^{k-1}},\ \boldsymbol{a}], Y(s + d + 1) = [\boldsymbol{b},\ P_{sd^{k-1}}]$.

This subcase can be dealt with in the same way as in the former one. We omit the details. $\square$

Because $(Q_s f(N)N^q)^k = Q_{s^k} \cdot \prod_{i=0}^{k-1}(N^{(q+1)s^i} + \cdots + N^{(q+d)s^i})$ (see [21–22]), we get that to solve (1.1) under the assumption $A = P^{\mathrm{T}}M$ for some permutation matrix P is equivalent to finding suitable q and s such that $d|s|d^{k-1}$, $\boldsymbol{s^k} = \mathbf{1}$, and $A_0 + A_1 + \cdots + A_{k-1} = Z_n \setminus \{\mathbf{0}\}$, where $A_i = \{(\mathbf{1} + \boldsymbol{q})\boldsymbol{s^i},\ (\mathbf{2} + \boldsymbol{q})\boldsymbol{s^i}, \ldots, (\boldsymbol{d} + \boldsymbol{q})\boldsymbol{s^i}\}$. We do not know whether the solution to the latter number-theoretical question must have $s = (-d)^t$ for some t.

3. Two corollaries

We give two direct applications of the preceding results in this section. We shall need the following result from [22,23]:

(★) In the set of matrices which are permutation similar to $Q_{(-d)^t}f(N)N^q$ for some t and q, all the distinct solutions A to (1.1), up to permutation similarity, are $Q_{(-d)^t}f(N)$, where $1 \leqslant t \leqslant k-1$ and $\gcd(t, k) = 1$.

Corollary 3.1. *If $A^k = J_{d^k+1} - I_{d^k+1}$ for a prime d, and A can be converted to M by permuting the rows, then the set of all distinct solutions A is* $\{Q_{(-d)^t}f(N) | 1 \leqslant t \leqslant k-1, \gcd(t,k) = 1\}$, *up to permutation similarity.*

Proof. As a result of Theorem 2.1, A must be of the form $Q_s f(N)N^q$, where $d|s|d^{k-1}$ and $\boldsymbol{s^k} = \mathbf{1}$. Since d is a prime and k is odd, the only possibility is that s is a power of $-d$. Hence the corollary follows from (★). $\square$

Corollary 3.2. *If $k = 3$ and $A = P^{\mathrm{T}}M$ for some permutation matrix P, then the set of all distinct solutions A to* (1.1) *is* $\{Q_{-d}f(N),\ Q_{(-d)^2}f(N)\}$ *up to permutation similarity.*

Proof. Let $s = -dt$, where $t|d$. If $1 < |t| < d$, then $1 < |t^3| < d^3$ and so it cannot hold $\boldsymbol{t^3} = \mathbf{1}$. But $\boldsymbol{s^3} = \boldsymbol{t^3}$, and then $\boldsymbol{s^3} \neq \mathbf{1}$ follows. When $|t| = 1$ or d, it is trivial to check that $\boldsymbol{s^3} = \mathbf{1}$ if and only if $s = -d$ or $(-d)^2$. Thus (★) gives our assertion. □

4. Partitionable graph

In this section, we study (1.1) with the language of graph theory. In particular, a partitionable graph approach is introduced. In view of Theorem 2.1, it may be of interest to know when the condition $A = P^{\mathrm{T}}M$ can be guaranteed. We set up some results in this direction, which will help us to obtain the complete solution of $A^k = J_{2^k+1} - I_{2^k+1}$.

First of all, there are some notations. $\omega_v(G)$, the local clique number at a vertex v of the graph G, is the size of the largest clique in G which contains v. $\omega(G)$, the clique number of G, is the greatest one among all $\omega_v(G)$'s for $v \in G$. Chvátal [13] defines a web C_m^t to be the graph whose vertices can be enumerated as $v_1, \ldots, v_m$ so that v_i is adjacent to v_j if and only if the indices i and j differ by at most t modulo m. In fact, C_m^t is just $(C_m)^t$, the tth power of the cycle $C_m = C_m^1$. Following Sebǒ [19], we say that a graph G is locally a web at a vertex v_0 if there exists an ordering $v_{-(\omega_0-1)}, \ldots, v_{-1}, v_0, v_1, \ldots, v_{\omega_0-1}$ of $2\omega_0 - 1$ distinct vertices so that $v_i, v_{i+1}, \ldots, v_{i+\omega_0-1}$ form a clique in G for $i = -(\omega_0 - 1), \ldots, 0$, where $\omega_0 = \omega_{v_0}(G)$. Although the concept of the web seems contrived at first sight, it really appears quite naturally in the study of perfect graph [6,12,13,19,20], and is also important in our investigation of (1.1). We denote the neighbor set of a vertex v in a graph G by $N_G(v)$. The following theorem is intuitively reasonable, but we cannot find a shorter proof.

Theorem 4.1. *A connected graph G of order m with every vertex in exactly ω cliques of size ω, and every edge in at least one clique of size ω, where $\omega = \omega(G) > 1$, is locally a web everywhere if and only if it is the web $C_m^{\omega-1}$.*

Proof. The 'if' part is trivial. So we turn to the 'only if' part.

We refer to the set of cliques of size ω in G containing a vertex v_i as $C(v_i)$. Since G is locally a web at v_i and $\omega_{v_i}(G) = \omega$, there are $2\omega - 1$ distinct vertices $v_i^{-(\omega-1)}, \ldots, v_i^{-1}, v_i^0 = v_i, v_i^1, \ldots, v_i^{\omega-1}$, such that $C_j = \{v_i^j, \ldots, v_i^{j+\omega-1}\} \in C(v_i)$ for $j = -(\omega - 1), \ldots, 0$. But we have $|C(v_i)| = \omega$ and every edge of G is in at least one clique of size ω. Thus it follows that $C(v_i) = \{C_{-(\omega-1)}, \ldots, C_0\}$ and $\{v_i\} \cup N_G(v_i) = \{v_i^{-(\omega-1)}, \ldots, v_i^{\omega-1}\}$. We now construct the labeled path $CP(v_i) = (C_{-(\omega-1)}, \ldots, C_0)$, which is the graph on labels $C_{-(\omega-1)}, \ldots, C_0$ with $C_jC_{j+1},\ j = -(\omega - 1), \ldots, -1$, as edge set. Observe that

$$|C_p \Delta C_q| = 2|p - q|, \tag{4.1}$$

where $-(\omega-1) \leqslant p,\ q \leqslant 0$. Clearly $CP(v_i)$ is just the path with the ω vertices labeled by the elements of $C(v_i)$ and with an edge between any two vertices for which the symmetric difference of their corresponding cliques in $C(v_i)$ is of cardinality 2. So $CP(v_i)$ is uniquely determined for v_i up to isomorphism. For convenience, we often refer to a vertex in a labeled graph just by calling its label alone. The structure of labeled graph is introduced here only to characterize the 'adjacent' relation among the set of labels. Next, taking $N_G(v_i) \cup \{v_i\}$ as the set of labels, we build another labeled path in the procedure below:

- Take a representation of $CP(v_i)$, say $(B_{-(\omega-1)}, \dots, B_0)$.
- Connect the only vertex in $B_i \setminus B_{i-1}$ to the only one in $B_{i-1} \setminus B_{i-2}$ for $i = -(\omega-3), \dots, 0$.
- Join the singleton in $B_i \setminus B_{i+1}$ to that in $B_{i+1} \setminus B_{i+2}$ for $i = -(\omega-1), \dots, -2$.
- Add an edge between the only two vertices in $\bigcap_{j=1}^{\omega-1} B_{j+t}$ for $t = -\omega$ and $-(\omega-1)$, respectively.

We cannot be sure whether it holds $B_i = C_i$ for $i = -(\omega-1), \dots, 0$ or $B_i = C_{-(\omega-1)-i}$ for $i = -(\omega-1), \dots, 0$, but the fact that the path $CP(v_i) = (C_{-(\omega-1)}, \dots, C_0) = (C_0, \dots, C_{-(\omega-1)})$ is determined up to isomorphism, really tells us that these are all the possible cases. Hence the intersection pattern of C_j's ensures that this procedure generates the same edge set on $N_G(v_i) \cup \{v_i\}$, and so results in the same path, whatever the case is. This fact merely reflects that the preceding order $v_i^{-(\omega-1)}, \dots, v_i^{\omega-1}$ can be recognized from $CP(v_i)$ up to order reversal. Let us designate this labeled path as $P(v_i)$, which is well-defined for each v_i.

Now we shall associate with G a new graph H, which is produced by 'gluing together' all the $P(v_i)$'s, as our proof will show. H has vertex set the same as G and edge set the pairs of vertices with exactly $\omega-1$ cliques of size ω in G including them both.

Pick arbitrarily a vertex v_i of G. Suppose $P(v_i) = (v_i^{-(\omega-1)}, \dots, v_i^{\omega-1})$, where $v_i = v_i^0$. The intersecting relation among the sets in $C(v_i)$ indicates $N_H(v_i) = \{v_i^{-1}, v_i^1\}$. Therefore we know that H is 2-regular and hence a disjoint union of cycles.

Let C_j represent the clique $\{v_i^j, \dots, v_i^{j+\omega-1}\}$ in G for $j = -(\omega-1), \dots, 0$. It is clear that $CP(v_i) = C_{-(\omega-1)}, \dots, C_0)$.

We claim that $P(v_i)$ is a subgraph of H in the sense that

$$E\left(H|_{\{v_i^{-(\omega-1)}, \dots, v_i^{\omega-1}\}}\right) \supseteq E(P(v_i)).$$

The case $\omega = 2$ is trivial. Assume $\omega > 2$ and hence $v_i^1 \in C_{-1}$ follows. We now turn our attention to $CP(v_i^{-1})$. Noting (4.1), we see that there are only two possibilities, $CP(v_i^{-1}) = (B,\ C_{-(\omega-1)}, \dots, C_{-1})$ or $(C_{-(\omega-1)}, \dots, C_{-1}, B)$, where B is the unique element in $C(v_i^{-1}) \setminus \{C_{-(\omega-1)}, \dots, C_{-1}\}$. If it occurs the latter case, then we conclude from $v_i^{-1} \notin C_0$ that $B \neq C_0$, henceforth $v_i \notin B$. But we have $v_i \in C_{-1}$ and $|C_{-1} \setminus B| = 1$. This shows $\{v_i\} = C_{-1} \setminus B$. Therefore $v_i^1 \in C_{-1}$

implies $v_i^1 \in B$. If ω is even greater than 3, then B, C_0, C_{-1}, C_{-2} are all in $CP(v_i^1)$. However, applying formula (4.1) to the graph $CP(v_i)$ and $CP(v_i^{-1})$, respectively, we get $|C_{-1} \Delta C_{-2}| = |C_{-1} \Delta C_0| = 2 = |C_1 \Delta B|$. It is impossible for C_{-1} cannot have degree greater than 2 in $CP(v_i^1)$. So we obtain $\omega = 3$ and hence $B = \{v_i^{-1}, v_i^1, u\}$ for some $u \notin \{v_i^j \,|\, j = \pm 1, 0\}$. At this moment, it is clear from the definition that the 3-cycle (v_i^0, v_i^1, v_i^{-1}) is a connected component of the 2-regular graph H. But the existence of the clique $\{v_i^0, v_i^1, v_i^2\}$ asserts that one of v_i^0 and v_i^1 should be adjacent to v_i^2 in H. A contradiction. Thus we see that only the former case can happen, that is, $CP(v_i^{-1}) = (B, C_{-(\omega-1)}, \ldots, C_{-1})$. Consequently there exists a vertex u such that $P(v_i^{-1}) = (u, v_i^{-(\omega-1)}, \ldots, v_i^{\omega-2})$. It in turn follows $\{v_i^{-1}, v_i^{-2}\} \in E(H)$. Repeating this process, we obtain that all the edges of $P(v_i)$ are also edges of H. It then justifies our assertion.

From the statement above, we deduce that the set of vertices $N_G(v_i) \cup \{v_i\} = V(P(v_i))$ is on one of the connected components of H. But G is connected. So it follows that the 2-regular graph H has only one connected component, and hence H is the cycle C_m^1. Moreover, the fact that every $P(v_i)$ is a subgraph of H and the vertex set of $P(v_i)$ is just $N_G(v_i) \cup \{v_i\}$ enables us to find out that G can be reconstructed from H by adding edges between those nonadjacent vertices at distance less than ω on it. This then implies $G = C_m^{\omega-1}$ as desired. $\square$

To proceed on, we introduce the concept of partitionable graph [3,6,9,12,13,19,20], which plays an important role in the investigation of perfect graph, and is also very attractive in its own right for the rich combinatorial property involved. Let $\alpha, \omega \geqslant 2$ be two integers. An (α, ω) partitionable graph G is a graph of order $\alpha\omega$+1 such that for every $v \in V(G)$ there is a partition of $V(G) \setminus \{v\}$ into α cliques of size ω and a partition of the same set into ω stable sets of size α. An (α, ω) partitionable graph is normalized provided every edge in it belongs to some clique of size ω. We shall make use of the following results contained in [6,11,12,19]. Let B and C be $m \times m$ $(0, 1)$ matrices. Then:

(a) $CB = J - I \Rightarrow BC = J - I$.

(b) $CB = J - I \Rightarrow$ There exist positive integers α, ω such that $JC = CJ = \alpha J$, $BJ = JB = \omega J$. Further, $G(BB^{\mathrm{T}})$ is a normalized (α, ω) partitionable graph when $\alpha, \omega \geqslant 2$. (Here we denote by $G(S)$ the graph with $\{0, 1, \ldots, m-1\}$ as the vertex set such that i is adjacent to j if and only if $i \neq j$ and $e_i S e_j^{\mathrm{T}} > 0$ for a symmetric matrix S of order m.)

(c) Every vertex of an (α, ω) partitionable graph is in exactly ω cliques of size ω.

(d) The clique number of an (α, ω) partitionable graph is ω.

(e) An (α, ω) partitionable graph is $(2\omega - 2)$-connected.

(We remark that we only need a weak form of (e), that is, partitionable graph is connected, which has a very simple proof from the definition of the partitionable graph given above.)

We are ready to apply Theorem 4.1 by now. The number in boldface means the corresponding residue class modulo m in Theorem 4.2 and its proof.

Theorem 4.2. *If $CB = J_m - I_m$ and $G(BB^{\mathrm{T}})$ is locally a web everywhere, then $\{B(i)\,|\,i = 1, 2, \ldots, m\} = \{\{q(\boldsymbol{i}), q(\boldsymbol{i}+\mathbf{1}), \ldots, q(\boldsymbol{i}+\boldsymbol{\omega}-\mathbf{1})\}\,|\,\boldsymbol{i} \in Z_m\}$ for some $\omega > 0$ and some permutation q on Z_m.*

Proof. We deduce from (a) that $BC = J_m - I_m$, and thus $C^{\mathrm{T}}B^{\mathrm{T}} = J_m - I_m$. (b) implies now there are some positive integers α, ω such that $C^{\mathrm{T}}J = JC^{\mathrm{T}} = \alpha J, B^{\mathrm{T}}J = JB^{\mathrm{T}} = \omega J$.

If $\alpha = 1$, then C is a permutation matrix and $B = C^{\mathrm{T}}(J - I)$ holds. It follows that B is obtained from $J - I$ by permuting the rows. So we can simply take q as the identical permutation on Z_m. If $\omega = 1$, then B is a permutation matrix, a trivial case again.

Assume henceforth $\alpha, \omega \geqslant 2$. As a result of (b), $C^{\mathrm{T}}B^{\mathrm{T}} = J_m - I_m$ implies now $G(BB^{\mathrm{T}})$ is a normalized (α, ω) partitionable graph. By noting (c), (d), (e) in addition, Theorem 4.1 allows us to conclude that $G(BB^{\mathrm{T}})$ is the web $C_m^{\omega-1}$. Let $\Gamma = \{\{\boldsymbol{i_1}, \boldsymbol{i_2}, \ldots, \boldsymbol{i_\omega}\}|0 \leqslant i_1 < i_2 < \cdots < i_\omega \leqslant m-1, B^{\mathrm{T}}(i_j) \cap B^{\mathrm{T}}(i_t) \neq \emptyset$ for all $j, t = 1, 2, \ldots, \omega\}$. It is not difficult to see that Γ corresponds to the set of ω-cliques in $G(B^{\mathrm{T}}B)$. Note that $C_m^{\omega-1}$ has one good property that it has precisely m cliques of size ω and these cliques distribute in a highly regular way. Expressing it in terms of the matrix B, we get the $|\Gamma| = m$ and there is some permutation q on Z_m such that the set Γ is just $\{\{q(\boldsymbol{i}), q(\boldsymbol{i}+\mathbf{1}), \ldots, q(\boldsymbol{i}+\boldsymbol{\omega}-\mathbf{1})\}|\boldsymbol{i} \in Z_m\}$. But it can be seen that $\Sigma = \{B(i)|i = 1, 2, \ldots, m\} \subseteq \Gamma$, because the (0,1) matrix B satisfies $BJ = \omega J$. Moreover, the nonsingularity of B implies $|\Sigma| = m = |\Gamma|$. So we conclude that $\Sigma = \Gamma$ and the proof is ended. $\square$

We specialize Theorem 4.2 to give the following result.

Theorem 4.3. *If $A^k = J_n - I_n$ and $G(AA^{\mathrm{T}})$ is locally a web everywhere, then A is permutation similar to $P^{\mathrm{T}}M$ for some permutation matrix P.*

Proof. To use Theorem 4.2, we should identify A^{k-1} with C and A with B. Let q be a permutation on Z_m satisfying Theorem 4.2 and Q and $n \times n$ permutation matrix with $Q(i) = q(\boldsymbol{i})$ for each i. Then Theorem 4.2 gives $\{QAQ^{\mathrm{T}}(i)\,|\,i = 1, 2, \ldots, n\} = \{\{\boldsymbol{i}, \boldsymbol{i}+\mathbf{1}, \ldots, \boldsymbol{i}+\boldsymbol{d}-\mathbf{1}\}\,|\,\boldsymbol{i} \in Z_n\} = \{M(i)\,|\,i = 1, 2, \ldots, n\}$. So QAQ^{T} can be transformed into M by permuting the rows. This means $QAQ^{\mathrm{T}} = P^{\mathrm{T}}M$ for some permutation matrix P, which is the result. $\square$

From the (0,1) matrix equation $A^k = J_{2^k+1} - I_{2^k+1}$, we certainly can deduce $(A^{\mathrm{T}})^k = J_{2^k+1} - I_{2^k+1}$. So (b) implies that $G(A^{\mathrm{T}}A)$ is a $(2^{k-1}, 2)$ partitionable graph. Hence every vertex of $G(A^{\mathrm{T}}A)$ is in exactly two cliques of size two, owing to (c). It then follows from (d) that $G(AA^{\mathrm{T}})$ is locally a web everywhere.

Thus we can derive the following theorem from Theorem 4.3 and Corollary 3.1.

Theorem 4.4. *The set of all distinct solutions A to the equation* $A^k = J_{2^k+1} - I_{2^k+1}$ *is* $\{Q_{(-2)^t} f(N) \mid \gcd(t,k) = 1, 1 \leqslant t \leqslant k-1\}$, *up to permutation similarity.*

We remark that Lam and Van Lint [18] have established our Theorem 4.4 in the special case $k=3$ by a completely different method.

By virtue of Theorem 4.3, it arises naturally the problem of recognizing the local web property. We have noticed the following:

- If G is (α, ω) partitionable, $v \in V(G)$, and $N(v)$ is covered by two $(\omega-1)$-cliques, then G is locally a web at v [19].
- *A conjecture of Ravindra*: For an (α, ω) partitionable graph G, if a vertex $v \in V(G)$ has exactly $2\omega - 2$ neighbors, then $N(v)$ can be covered by two $(\omega-1)$-cliques [19].
- If G is an (α, ω) partitionable claw-free graph, then $|N(v)| = 2\omega - 2$ for all $v \in V(G)$ [9].

These information illustrate that if the conjecture of Ravindra can be proved true, then our discussion about (1.1) in this paper may be valid under the assumption $G(A^{\mathrm{T}}A)$ is claw-free. We do not know whether the claw-free property of $G(A^{\mathrm{T}}A)$ is a direct consequence of (1.1). It is also not clear whether the concept of completely positive matrix [4] has any connection with the discussion of (1.1). We hope that the rich results developed in the study of perfect graph and completely positive matrix may be helpful in the further research on this topic.

Acknowledgements

The authors are grateful to the referee for careful reading which has greatly improved the readability of this paper. Y. Wu thanks Minqiang Yu for friendly help of all kinds. He is also indebted to Prof. Sebŏ for sending him several papers on perfect graph. Q. Li is supported in part by the NNSF of China.

References

[1] N. Alon, R.A. Brualdi, B.L. Shader, Multicolored forests in bipartite decompositions of graphs, J. Combin. Theory B 53 (1991) 143–148.

[2] E.T. Baskoro, M. Miller, J. Plesnik, Š. Znám, Digraphs of degree 3 and order close to the Moore bound, J. Graph Theory 20 (1995) 339–349.

[3] C.Berge, V.Chvátal, Topics on Perfect Graphs, Annals Of Discrete Mathematics, vol. 21, Elsevier, Amsterdam, 1984.

[4] A.Berman, Completely positive graphs, in: R.A. Brualdi, S. Friedland, V. Klee (Eds.), Combinatorial and Graph-Theoretical Problems in Linear Algebra, IMA vol. Math. Appl. 50, Springer, New York, 1993, pp. 229–233.
[5] J.C. Bermond, F.Ö. Ergincan, Bus interconnection networks, Disc. Appl. Math. 68 (1996) 1–15.
[6] R.G. Bland, H.C. Huang, L.E. Trotter, Graphical properties related to minimal imperfection, Disc. Math. 27 (1979) 11–22.
[7] W.G. Bridges, H.J. Ryser, Combinatorial design and related systems, J. Algebra 13 (1969) 432–446.
[8] R.A. Brualdi, H.J. Ryser, Combinatorial Matrix Theory, Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 1991.
[9] M.A. Buckingham, M.C. Golumbic, Partitionable graphs, circle graphs, and the Berge strong perfect graph conjecture, Disc. Math. 44 (1983) 45–54.
[10] D. de Caen, D.A. Gregory, I.P. Hughes, D. Kreher, Near factors of finite groups, Ars Combin. 29 (1990) 53–63.
[11] D. de Caen, D.A. Gregory, On the decomposition of a directed graph into complete bipartite subgraphs, Ars Combin. 23 (1987) 139–146.
[12] V. Chvátal, R.L. Graham, A.F. Perold, S.H. Whitesides, Combinatorial designs related to the strong perfect graph conjecture, Disc. Math. 26 (1979) 83–92.
[13] V. Chvátal, On the strong perfect graph conjecture, J. Combin. Theory B 20 (1976) 139–141.
[14] P.J. Davis, Circulant Matrices, Wiley, New York, 1979.
[15] F. Ergincan, D.A. Gregory, Directed Moore hypergraphs, Disc. Appl. Math. 63 (1995) 117–127.
[16] A.J. Hoffman, M.H. McAndrew, The polynomial of a directed graph, Proc. Amer. Math. Soc. 16 (1965) 303–309.
[17] C.W.H. Lam, S. Swiercz, L. Thiel, E. Regener, A computer search for (α, ω) graphs, Congr. Numer. 27 (1990) 285–289.
[18] C.W.H. Lam, J.H. Van Lint, Directed graphs with unique paths of fixed length, J. Combin. Theory B 24 (1978) 331–337.
[19] A. Sebŏ, The connectivity of minimal imperfect graphs, J. Graph Theory 23 (1996) 77–85.
[20] A. Sebŏ, On critical edges in minimal imperfect graphs, J. Combin. Theory B 67 (1996) 62–85.
[21] Y. Wu, Q. Li, On the matrix equation $A^k + A^{k+l} = J_n$, Linear Algebra Appl. 277 (1998) 41–48.
[22] Y. Wu, Q. Li, Some results on consecutive-d digraphs, submitted.
[23] Y. Wu, Q. Li, A class of digraphs with unique paths of fixed length, in preparation.
[24] Y. Wu, Q. Li, J. Li, Spectra and elementary cycles of the digraphs with unique paths of fixed length, Linear Algebra Appl. 293 (1999) 145–158.