NORTH-HOLLAND

A Bound on the Exponent of Primitivity in Terms of Diameter

Jian Shen
Department of Mathematics
University of Science and Technology of China
Hefei, Anhui, 230026, The People's Republic of China

Submitted by Richard A. Brualdi

ABSTRACT

An $n \times n$ nonnegative matrix A is called primitive if for some positive integer k, every entry in A^k is positive ($A^k \gg 0$). The exponent of primitivity of A is defined to be $\gamma(A) = \min\{k \in Z_+ : A^k \gg 0\}$, where Z_+ denotes the set of positive integers. Two conjectures due to Hartwig, Neumann, and Lin in 1984 or so are that $\gamma(A) \leqslant (m-1)^2 + 1$ and $\gamma(A) \leqslant D^2 + 1$, where m is the degree of the minimal polynomial of A and D is the diameter of the directed graph of A. It is well known that the latter is stronger than the former because $D \leqslant m - 1$. In a recent paper we have proved $\gamma(A) \leqslant (m-1)^2 + 1$; in this paper we prove the conjecture $\gamma(A) \leqslant D^2 + 1$ on that basis.

1. INTRODUCTION AND NOTATION

For all terminology and notation used here we follow [1].

Associated with an $n \times n$ nonnegative matrix $A = (a_{ij})$ we shall consider its directed graph $D(A)$, which consists of a set V of n vertices, labeled conveniently, $1, 2, \dots, n$, and a set of directed edges E with a directed edge from vertex i to vertex j if and only if $a_{ij} \neq 0$. We shall use the notation $i \to j$ and $i \nrightarrow j$ to denote, respectively, that there is a directed edge from vertex i to vertex j and that there is no such edge. Similarly, $i \xrightarrow{d_1, \dots, d_s} j$ and $i \xrightarrow{d_1, \dots, d_s}\!\!\!\!\!\!\!/\;\; j$ denote, respectively, that there are paths of lengths $d_1, \dots, d_s$ connecting vertex i to vertex j, and that there are no such paths. The

655 Avenue of the Americas, New York, NY 10010
0024-3795/96/$15.00
SSDI 0024-3795(94)00205-R

distance $d(i,j)$ from vertex i to vertex j is the minimal length of a path linking vertex i to vertex j. By D and D_{A^k} we denote, respectively, the diameter of $D(A)$ and the diameter of $D(A^k)$. Note the following fact:

$$A^k \gg 0 \quad \Leftrightarrow \quad i \xrightarrow{k} j \quad \text{for any } i,j \in V(D(A)).$$

Thus, in particular, if $(A^k)_{ii} > 0$, then the vertex i lies on a closed path of length k in $D(A)$.

Suppose $a_0, \dots, a_s$ is a set of distinct positive integers with $\gcd(a_0, \dots, a_s) = 1$. Then we define $\Phi(a_0, \dots, a_s)$ to be the least integer m such that every integer $k \geqslant m$ can be expressed in the form $k = c_0 a_0 + \cdots + c_s a_s$, where $c_0, \dots, c_s$ are some nonnegative integers. A well-known result due to Schur shows that $\Phi(a_0, \dots, a_s)$ is well defined when $\gcd(a_0, \dots, a_s) = 1$.

2. SOME LEMMAS

LEMMA 2.1 [4]. *Let* $0 < a_0 < a_1 < \cdots < a_s$, $s \geqslant 2$, *and* $\gcd(a_0, a_1, \dots, a_s) = 1$. *If it is impossible to choose* a_l *and* a_m *from the set* $\{a_0, a_1, \dots, a_s\}$ *such that for any* $0 \leqslant i \leqslant s$, a_i *can be expressed in the form* $a_i = c_{i_1} a_l + c_{i_2} a_m$, *where* c_{i_1}, c_{i_2} *are some nonnegative integers, then*

$$\Phi(a_0, a_1, \dots, a_s) \leqslant \lfloor \tfrac{1}{2} a_0 \rfloor (a_s - 2).$$

LEMMA 2.2 [4]. *Suppose* $\gcd(a_0, a_1, \dots, a_s) = 1$. *For each residue class modulo* a_0 *choose its least representative, expressible as* $a_1\alpha_1 + a_2\alpha_2 + \cdots + a_s\alpha_s$, *with* $\alpha_1, \alpha_2, \dots, \alpha_2$ *nonnegative integers. Choose the maximal one of these representatives,* $a_1\beta_1 + a_2\beta_2 + \cdots + a_s\beta_s$. *Then*

$$\Phi(a_0, a_1, \dots, a_s) = a_1\beta_1 + a_2\beta_2 + \cdots + a_s\beta_s - a_0 + 1.$$

DEFINITION 2.1 [3]. Let $(Z_{a_0}, +) = \{0, 1, \dots, a_0 - 1\}$ be the finite Abelian group with the operation $+$ modulo a_0. Suppose $A \subset Z_{a_0}$ and $1 \neq d \mid a_0$. We define $A(\text{mod } d) = \{a \in Z_d : \text{there exists } a_1 \in A \text{ such that } a \equiv a_1 \pmod{d}\}$, so $A(\text{mod } d) \subset Z_d$.

DEFINITION 2.2 [3]. Suppose $A, B \subset Z_{a_0}$. We define $A + B = \{a + b \in Z_{a_0} : a \in A,\ b \in B\}$, and $|A|$ denotes the number of elements in A.

LEMMA 2.3 [3]. *Suppose* $\gcd(a_0, a_1, a_2) = 1$, $0 < a_0 < a_1 < a_2 < a_3$, *and* $a_i \not\equiv a_j \pmod{a_0}$ *for any* $i \neq j$. *Let* $A = \{0, a_1, a_2, a_3\} \subset Z_{a_0}$ *and* $K = \lfloor (a_0 - 2)/3 + 1 \rfloor = (a_0 - 1 + l)/3$, *where* $0 \leqslant l \leqslant 2$. *Then*:

(1) *If both* $2 \mid a_0$ *and* $|A(\bmod a_0/2)| = 2$, *then* $\Phi(a_0, a_1, a_2, a_3) \leqslant a_2(a_0/2 - 2) + a_3 - a_0 + 1$.

(2) *If either* $2 \mid a_0 + 1$ *or* $|A(\bmod a_0/2)| \geqslant 3$, *then*

$$\Phi(a_0, a_1, a_2, a_3) \leqslant (K - l)a_3 + la_2 - a_0 + 1$$

$$= \begin{cases} \dfrac{a_0 - 1}{3}(a_3 - 3), & 3 \mid a_0 - 1, \\ \left(\dfrac{a_0}{3} - 1\right)a_3 + a_2 - a_0 + 1, & 3 \mid a_0, \\ \left(\dfrac{a_0 + 1}{3} - 2\right)a_3 + 2a_2 - a_0 + 1, & 3 \mid a_0 + 1. \end{cases}$$

LEMMA 2.4 [3]. *Suppose* $\gcd(a_0, a_1, a_2) = 1$ *and* $a_i \neq a_j \pmod{a_0}$ *for any* $i \neq j$. *If* $a_2 + 2a_1 \equiv 0 \pmod{a_0}$ *and also there exist positive integers* l_1 *and* l_2 *such that* $a_2 l_2 \equiv a_1 l_1 \pmod{a_0}$, *then*

$$\Phi(a_0, a_1, a_2) \leqslant \max((l_2 - 1)a_2 + a_1, (l_1 + 1)a_1) - a_0 + 1,$$

$$\Phi(a_0, a_1, a_2) \leqslant \max(l_2 a_2 + a_1, (l_1 - 1)a_1) - a_0 + 1.$$

3. THE PROOF OF THE CONJECTURE $\gamma(A) \leqslant D^2 + 1$

In [2] the only case for which we cannot prove the conjecture $\gamma(A) \leqslant D^2 + 1$ is that when $D(A)$ satisfies the following hypothesis

(*) The length of the shortest circuit in $D(A)$ is $s = D + 1$; the diameter of $D(A^{D+1})$ is D; for any $A_0, A_D \in V(D(A))$ such that $A_0 \overset{D^2 - 1}{\not\longrightarrow} A_D$ there exists some $k = k(A_0, A_D)$, $1 \leqslant k \leqslant D$, $\gcd(k, D + 1) = 1$, such that

$$A_0 \xrightarrow{D+1, k} A_1 \xrightarrow{D+1, k} A_2 \xrightarrow{D+1, k} \cdots \xrightarrow{D+1, k} A_D,$$

and for any k' such that $k' \neq k$, $1 \leqslant k' \leqslant D$, we always have $A_{i-1} \overset{k'}{\nrightarrow} A_i$ for any $1 \leqslant i \leqslant D$.

Therefore in this paper it is sufficient for us to prove $\gamma(A) \leqslant D^2 + 1$ under hypothesis (*).

DEFINITION 3.1. Let

$$M = \left\{ a \in V(D(A)) : \text{there exists some } b \in V(D(A)) \text{ such that } a \overset{D^2-1}{\not\longrightarrow} b \right\},$$

$$G(a) = \left\{ k : 1 \leqslant k \leqslant D \text{ and there exists some } b \in V(D(A)) \text{ such that } a \xrightarrow{D+1,\,k} b \right\},$$

$$L(a) = \{ c : a \in V(D(A)) \text{ lies on a closed path with the length } c \},$$

$$L'(a) = \{ c \in L(a) : D + 1 < c < 2(D+1) \}.$$

By hypothesis (*), we know $D + 1 \in L(a)$ and $D + 1 \leqslant c$ for any $c \in L(a)$.

Suppose $a \in V(D(A))$. We define $\deg^+ a = |\{b \in V(D(A)) : a \to b\}|$.

THEOREM 3.1. *Suppose $a \in M$, $b \in V(D(A))$. Then:*

(1) *For any $k \in G(a)$, there exist some $c_1, c_2 \in L(a)$ such that $D + 1 \leqslant c_1 < c_2 < 2(D+1)$ and $c_2 - c_1 = D + 1 - k$.*

(2) *Suppose $a \to b$. If $\deg^+ a = 1$, then $1 \notin G(a)$. If $\deg^+ a > 1$, then there exists some integer l, $2 \leqslant l \leqslant D + 1$, such that $a \xrightarrow{l} b$.*

(3) *If $a \xrightarrow{D} b$, then there exists some $k \in G(a)$ such that $a \xrightarrow{D+(D+1-k)} b$.*

(4) *If $c \in L(a)$, then there exists some $k \in G(a)$ such that $c + (D + 1 - k) \in L(a)$.*

Proof. (1): Since $k \in G(a)$, by the definition of $G(a)$ there exists some $b \in (V(D(A))$ such that $a \xrightarrow{D+1,\,k} b$, so $a \neq b$ [otherwise, $D + 1 > k \in L(a)$, which is a contradiction]. Let $d = d(b, a)$, where $1 \leqslant d \leqslant D$; therefore $k + d$, $D + 1 + d \in L(a)$, and $D + 1 \leqslant k + d < D + 1 + d < 2(D + 1)$.

(2): If $\deg^+ a > 1$, then there exists some $c \in V(D(A))$ such that $a \to b$, $a \to c$, and $b \neq c$. Let $d = d(c, b)$, where $1 \leqslant d \leqslant D$; then $a \to c \xrightarrow{d} b$, i.e., $a \xrightarrow{1+d} b$, where $2 \leqslant 1 + d \leqslant D + 1$.

If $\deg^+ a = 1$, then for any $k \in G(a)$ there exists some $b' \in V(D(A))$ such that $a \xrightarrow{D+1,k} b'$, so $a \to b \xrightarrow{D,k-1} b'$, because $\deg^+ a = 1$. If $k = 1$, then $b = b'$ and $D \in L(a)$, which is a contradiction. Therefore $1 \notin G(a)$.

(3): Since $a \xrightarrow{D} b$, we suppose $a = a_0 \to a_1 \to \cdots \to a_{D-1} \to a_D = b$.

Firstly, we prove $\deg^+ a_i > 1$ for some i, $0 \leqslant i \leqslant D - 1$. For, if $\deg^+ a_i = 1$ for every i, $0 \leqslant i \leqslant D - 1$, then for any $b' \in V(D(A))$ such that $b \to b'$, it must be that $a = b'$, because $d(a, b') > D$ if $a \neq b'$, so $\deg^+ b = 1$ and $b \to a$. It is easy to prove that $D(A)$ cannot be primitive.

So we can choose t, $0 \leqslant t \leqslant D - 1$, such that $\deg^+ a_t > 1$ and $\deg^+ a_i = 1$ for any $i \leqslant t - 1$. By (2) we can choose the least l such that $2 \leqslant l \leqslant D + 1$ and $a_t \xrightarrow{l} a_{t+1}$.

Secondly, we prove $t + l \leqslant D + 1$. Otherwise, we suppose $t + l \geqslant D + 2$; then there exists some $c \in V(D(A))$ such that

$$a \xrightarrow{t} a_t \xrightarrow{D+1-t} c \xrightarrow{l-(D+1-t)} a_{t+1}.$$

If $a = c$, then $a \xrightarrow{l-(D+1-t)} a_{t+1}$. Noting that $d(a, a_{t+1}) = t + 1$, we have $l - (D + 1 - t) \geqslant t + 1$, contradicting $l \leqslant D + 1$. So $a \neq c$. Let $d = d(a, c)$, where $1 \leqslant d \leqslant D$. Since $a \xrightarrow{d} c$, $a_t \neq c$, and $\deg^+ a_i = 1$ for any $i \leqslant t - 1$, we have $d \geqslant t + 1$ and

$$a \xrightarrow{t} a_t \xrightarrow{d-t} c \xrightarrow{l-(D+1-t)} a_{t+1},$$

i.e., $a_t \xrightarrow{d+l-(D+1)} a_{t+1}$, but $2 \leqslant t + 1 + l - (D + 1) \leqslant d + l - (D + 1) < l$, contradicting the choice of l.

So $t + l \leqslant D + 1$, and there exists some $c' \in V(D(A))$ such that

$$a \xrightarrow{t} a_t \xrightarrow{1,l} a_{t+1} \xrightarrow{D+1-(t+l)} c' \xrightarrow{l-2} a_D = b,$$

i.e., $a \xrightarrow{D+1,\,D+2-l} c'$. Then there exists some $k \in G(a)$ such that $k = D + 2 - l$. Since $a \xrightarrow{D+1+l-2} a_D$, then $a \xrightarrow{D+(D+1-k)} b$.

(4): Since $D + 1 \leqslant c \in L(a)$, there exists some $b \in V(D(A))$ such that $a \xrightarrow{D} b \xrightarrow{c-D} a$. By (3) there exists some $k \in G(a)$ such that $a \xrightarrow{D+(D+1-k)} b \xrightarrow{c-D} a$, i.e., $c + D + 1 - k \in L(a)$. Therefore Theorem 3.1 follows. ■

Now we know if $a \in M$, then by hypothesis (*) there exists at least one $k \in G(a)$ such that $\gcd(D + 1, k) = 1$. Note that $D + 1 \in L(a)$; then $L'(a) \neq \varnothing$ because of Theorem 3.1(4). Furthermore, by Theorem 3.1(1) we can prove $\gcd(\{D + 1\} \cup L'(a)) = 1$, so $\Phi(\{D + 1\} \cup L'(a))$ is well defined. Next we will prove the conjecture according to $|L'(a)|$.

THEOREM 3.2. *Suppose* $a \in M$ *and* $|L'(a)| = 1$. *Then* $a \xrightarrow{D^2+1} b$ *for any* $b \in V(D(A))$.

Proof. Since $|L'(a)| = 1$, by Theorem 3.1(1) we have $|G(a)| = 1$. Let $G(a) = \{k\}$; then by hypothesis (*), we have $\gcd(D+1, k) = 1$. Noting that $D + 1 \in L(a)$, by Theorem 3.1(4) we have

$$D + 1 + i(D + 1 - k) \in L(a) \qquad \text{for any } i \text{ such that} \quad 0 \leqslant i \leqslant D. \quad (1)$$

Case 1: $k \geqslant 2$. By Roberts's formula [5], we have

$$\begin{aligned}\Phi(L(a)) &\leqslant \Phi\big(D + 1, 2(D + 1) - k, 3(D + 1) - 2k, \dots, \\ &\qquad\qquad (D + 1)^2 - Dk\big) \\ &= \left\lfloor \frac{D + 1 - 2}{D} + 1 \right\rfloor (D + 1) + D(D - k) \\ &\leqslant D^2 - D + 1,\end{aligned}$$

from which $a \xrightarrow{D^2+1} b$ follows.

Case 2: $k = 1$. There exists some $b \in V(D(A))$ such that $a \xrightarrow{D+1,1} b$, i.e., $a \to b$ and $a \to a_1 \to a_2 \to \cdots \to a_D \to b$. Let $d = d(a_D, a)$ be such that $1 \leqslant d \leqslant D$; then $a \xrightarrow{D} a_D \xrightarrow{d} a$, i.e., $2D + 1 > D + d \in L(a)$. Since $|L'(a)| = 1$, from (1) we have $L'(a) = \{2D + 1\}$, so $D + d = D + 1$, i.e., $d = 1$ and $a_D \to a$. Noting that $a_D \to b$, it is easy to prove $b \xrightarrow{D} a_D$. Therefore we have $a \to b \xrightarrow{D} a_D \to a$, i.e., $D + 2 \in L'(a)$. Since $|L'(a)| = 1$, we know $2D + 1 = D + 2$, i.e., $D = 1$, so $D(A)$ is a complete graph and $a \xrightarrow{D^2+1} b$ is true. ■

THEOREM 3.3. *Suppose* $a \in M$ *and* $|L'(a)| \geqslant 3$. *Then* $a \xrightarrow{D^2} b$ *for any* $b \in V(D(A))$.

Proof. Suppose $c_1, c_2, c_3 \in L'(a)$ and $D + 1 < c_1 < c_2 < c_3 < 2(D + 1)$. By Lemma 2.3, we can prove $\Phi(D + 1, c_1, c_2, c_3) \leqslant D^2 - D$, from which $a \xrightarrow{D^2} b$ follows. ■

DEFINITION 3.2. For some given $a \in M$, by hypothesis (*) we can choose $K \in G(a)$ such that $\gcd(D + 1, K) = 1$ and

$$a = A_0 \xrightarrow{D+1,\,K} A_1 \xrightarrow{D+1,\,K} \cdots \xrightarrow{D+1,\,K} A_D,$$

where $A_i \neq A_j$ for any $i \neq j$. We consider K as the constant of a. Now for any $1 \leqslant i \leqslant D$ we define

$$l_i = d(A_i, a),$$

$$B_i = \{l_i + iK + j(D + 1 - K) : 0 \leqslant j \leqslant i\}.$$

It is easy to see that $\bigcup_{i=1}^{D} B_i \subset L(a)$.

THEOREM 3.4. *Suppose $a \in M$ and $|L'(a)| = 2$. If $2 \leqslant D \leqslant 5$, then $a \xrightarrow{D^2+1} b$ for any $b \in V(D(A))$.*

Proof. Suppose $L'(a) = \{c_1, c_2\}$ and $D + 1 < c_1 < c_2 < 2(D + 1)$. For any possible c_1 and c_2 we compute $\Phi(D + 1, c_1, c_2)$ to check if $\Phi(D + 1, c_1, c_2) \leqslant D^2 - D + 1$ is true.

Case 1: $D = 2$. Then $\Phi(3, 4, 5) = 3 = D^2 - D + 1$, so $a \xrightarrow{D^2+1} b$ follows.

Case 2: $D = 3$. There are two special cases.

Subcase 2.1: $c_1 = 5$, $c_2 = 6$, and $a \xrightarrow{3} b$. By Theorem 3.1(3), there exists some l such that $4 \leqslant l \leqslant 6$ and $a \xrightarrow{l} b$. We can check that $a \xrightarrow{10} b$ for any $4 \leqslant l \leqslant 6$.

Subcase 2.2: $c_1 = 6$, $c_2 = 7$, and $a \to b$. If $\deg^+ a > 1$, then by Theorem 3.1(2) there exists some l such that $2 \leqslant l \leqslant 4$ and $a \xrightarrow{l} b$. We can check $a \xrightarrow{10} b$ for any $2 \leqslant l \leqslant 4$.

If $\deg^+ a = 1$, then by Theorem 3.1(2) we have $1 \notin G(a)$, so only $K = 3$ can satisfy $\gcd(D + 1, K) = 1$ in Definition 3.2. We consider $B_2 = \{l_2 + 6, l_2 + 7, l_2 + 8\}$, defined in Definition 3.2, where $1 \leqslant l_2 \leqslant 3$, so $9 \in B_2 \subset L(a)$ for any $1 \leqslant l_2 \leqslant 3$; therefore

$$a \xrightarrow{9} a \to b, \qquad \text{i.e.,} \quad a \xrightarrow{10} b.$$

Case 3: $D = 4$. There are two special cases.

Subcase 3.1: $c_1 = 6$, $c_2 = 9$, and $a \xrightarrow{4} b$. Similarly to subcase 2.1, we can check that $a \xrightarrow{17} b$.

Subcase 3.2: $c_1 = 7$, $c_2 = 9$, and $a \xrightarrow{4} b$. By Theorem 3.1(1), we have $G(a) \subset \{1, 3\}$; by Theorem 3.1(3), we have $a \xrightarrow{6} b$ or $a \xrightarrow{8} b$. Using Theorem 3.1(3) again, we have $a \xrightarrow{8} b$ or $a \xrightarrow{10} b$, so $a \xrightarrow{17} b$ is always true.

Case 4: $D = 5$. There are four special cases.

Subcase 4.1: $c_1 = 10$, $c_2 = 11$, and $a \to b$. Similarly to subcase 2.2, we have $a \xrightarrow{26} b$.

Subcase 4.2: $c_1 = 9$, $c_2 = 11$, and $a \rightarrow b$; subcase 4.3: $c_1 = 8$, $c_2 = 11$, and $a \xrightarrow{5} b$; subcase 4.4: $c_1 = 9$, $c_2 = 10$, and $a \xrightarrow{3} b$. We consider B_3 if $K = 1$ and consider B_2 if $K = 5$. We can check that $a \xrightarrow{26} b$ is always true. ■

THEOREM 3.5. *If $D \geqslant 6$, $1 \leqslant l \leqslant D$, and $\gcd(l, D + 1) = 1$, then*

$$\Phi(D + 1, D + 1 + l, 2(D + 1) - l) \leqslant D^2 - D.$$

Proof. By Lemma 2.1, it is sufficient for us to consider $1 \leqslant l \leqslant 3$. Furthermore, if $2 \leqslant l \leqslant 3$ then $2 \mid D + 1$.

It is easy to see that $D + 1$, $D + 1 + l$, $2(D + 1) - l$, and $2(D + 1) + 2l$ satisfy the conditions of Lemma 2.3(2). Then

$$\begin{aligned} &\Phi(D + 1, D + 1 + l, 2(D + 1) - l) \\ &= \Phi(D + 1, D + 1 + l, 2(D + 1) - l, 2(D + 1) + 2l) \\ &\leqslant \begin{cases} \frac{D}{3}[2(D + 1) + 2l - 3], & 3 \mid D, \\ \left(\frac{D + 1}{3} - 1\right)[2(D + 1) + 2l] + 2(D + 1) - l - D, & 3 \mid +1, \\ \left(\frac{D + 2}{3} - 2\right)[2(D + 1) + 2l] + 2(2(D + 1) - l) - D, & 3 \mid D + 2, \end{cases} \\ &\leqslant D^2 - D. \end{aligned}$$

■

THEOREM 3.6. *Suppose $D > 6$, $1 \leqslant K \leqslant D$, and $\gcd(D + 1, K) = 1$. If $c_1 = 2(D + 1) - K$, $c_2 \equiv 2K \pmod{D + 1}$, and $D + 1 < c_2 < 2(D + 1)$, then*

$$\Phi(D + 1, c_1, c_2) \leqslant D^2 - D + 1.$$

Proof. If $D = 6, 7$, we can check for any possible c_1 and c_2 that $\Phi(D + 1, c_1, c_2) \leqslant D^2 - D + 1$. So we suppose $D \geqslant 8$, it is easy to prove $c_1 \neq c_2$.

Case 1: $c_1 < c_2$. Since $c_2 + 2c_1 \equiv 0 \pmod{D+1}$ and

$$\frac{D+1}{3}c_2 \equiv \frac{D+1}{3}c_1 \pmod{D+1}, \qquad 3 \mid D+1,$$

$$\frac{D+3}{3}c_2 \equiv \frac{D-3}{3}c_1 \pmod{D+1}, \qquad 3 \mid D,$$

$$\frac{D+2}{3}c_2 \equiv \frac{D-1}{3}c_1 \pmod{D+1}, \qquad 3 \mid D+2,$$

by Lemma 2.4 we have

$$\begin{aligned}\Phi(D+1, c_1, c_2) &\leqslant \max\left(\left(\frac{D+3}{3} - 1\right)c_2 + c_1, \left(\frac{D+1}{3} + 1\right)c_1\right) - D \\ &\leqslant \max\left(\frac{D}{3}(2D+1) + 2D, \frac{D+4}{3}2D\right) - D \\ &\leqslant D^2 - D.\end{aligned}$$

Case 2: $c_1 > c_2$. Similarly, since

$$\frac{D+1}{3}c_2 \equiv \frac{D+1}{3}c_1 \pmod{D+1}, \qquad 3 \mid D+1,$$

$$\frac{D}{3}c_2 \equiv \frac{D+3}{3}c_1 \pmod{D+1}, \qquad 3 \mid D,$$

$$\frac{D-1}{3}c_2 \equiv \frac{D+5}{3}c_1 \pmod{D+1}, \qquad 3 \mid D+2,$$

by Lemma 2.4 we have

$$\begin{aligned}\Phi(D+1, c_1, c_2) &\leqslant \max\left(\left(\frac{D+5}{3} - 1\right)c_1, \frac{D+1}{3}c_2 + c_1\right) - D \\ &\leqslant \max\left(\frac{D+2}{3}c_1, \left(\frac{D+1}{3} - \frac{1}{2}\right)c_2 + \tfrac{1}{2}(5D+5)\right) - D \\ &\leqslant D^2 - D.\end{aligned}$$

■

THEOREM 3.7. *Suppose* $D \geqslant 6$, $1 \leqslant K \leqslant D$, *and* $\gcd(D+1, K) = 1$. *If* $a \in M$ *and* $L'(a) = \{c_1, c_2\}$, *where* $c_1 \equiv -t_1 K \pmod{D+1}$, $c_2 \equiv -t_2 K \pmod{D+1}$, $t_1 \neq t_2$, *and* $\{t_1, t_2\} \subset \{1, 2, 3\}$, *then*

$$\Phi(L(a)) \leqslant D^2 - D.$$

Proof. Without loss of generality, we just prove this theorem under the condition that $t_1 = 1$ and $t_2 = 2$; the other cases can be proved similarly. It is easy to prove $c_1 \neq c_2$.

Case 1: $c_1 < c_2$. Then $c_1 = 2(D+1) - K$, $c_2 = 3(D+1) - 2K$, and $K \geqslant (D+2)/2$. Since $c_2 \in L'(a)$, by Theorem 3.1(1) we have $G(a) \subset \{K, 2K - (D+1)\}$. By Theorem 3.1(4), then $c_2 + (D + 1 - K) \in L(a)$ or $c_2 + 2(D + 1 - K) \in L(a)$.

Subcase 1.1: $c_3 = c_2 + (D + 1 - K) \in L(a)$. Then by Roberts's formula [5],

$$\Phi(D+1, c_1, c_2, c_3) = \left\lfloor \frac{D-1}{3} + 1 \right\rfloor (D+1) + D(D-K) \leqslant D^2 - D.$$

Subcase 1.2: $c_3 = c_2 + 2(D + 1 - K) \in L(a)$. Note the following fact: For any integer m such that $0 \leqslant m \leqslant D$, there exist nonnegative integers x, y, and z such that $x + 2y + 4z \equiv m \pmod{D+1}$ and $x + y + z \leqslant (D-3)/4 + 2$. By Lemma 2.2, using the method of [4, 3], we have

$$\Phi(D+1, c_1, c_2, c_3)$$
$$\leqslant \begin{cases} \dfrac{D-3}{4} c_3 + c_2 + c_1 - D, & 4 \mid D-3, \\ \dfrac{D-2}{4} c_3 + c_2 - D, & 4 \mid D-2, \\ \dfrac{D-1}{4} c_3 + c_1 - D, & 4 \mid D-1, \\ \max\left(\dfrac{D}{4} c_3, \dfrac{D-4}{4} c_3 + c_2 + c_1 \right) - D, & 4 \mid D, \end{cases}$$
$$\leqslant D^2 - D.$$

Case 2: $c_1 > c_2$. Then $c_1 = 2(D+1) - K$ and $c_2 = 2(D+1) - 2K$. By Lemma 2.1, it is sufficient for us to consider $K = 1, 3$; furthermore, if $K = 3$ then $2 \mid D + 1$.

Subcase 2.1: $K = 3$ and $2 \mid D + 1$. By Brauer's bound [6], then

$$\Phi(D+1, 2D-4, 2D-1) \leqslant \frac{D+1}{2}(2D-4) + 2(2D-1) + 1 - (5D-4) \leqslant D^2 - D.$$

Subcase 2.2: $K = 1$. Then $c_1 = 2D + 1$, $c_2 = 2D$, so we can suppose $a \to a_1 \to a_2 \to \cdots \to a_{D+1} \to \cdots \to a_{2D-1} \to a$ is the closed path with length $2D$. It is easy to prove $a \neq a_{D+1}$. Let $d = d(a, a_{D+1})$, where $1 \leqslant d \leqslant D$; then a lies on a closed path whose length is $D - 1 + d < 2D$. Since $L'(a) = \{2D, 2D+1\}$, we have $D - 1 + d = D + 1$, i.e., $d = 2$ and $a \xrightarrow{2} a_{D+1}$. Similarly we can prove $a_{d-1} \xrightarrow{2} a$. Note that $a_{D-1} \to a_D \to a_{D+1}$; then

$$a_{D+1} \xrightarrow{D} a_D \xrightarrow{D} a_{D-1}.$$

Therefore we have

$$a \xrightarrow{2} a_{D+1} \xrightarrow{D} a_D \xrightarrow{D} a_{D-1} \xrightarrow{2} a,$$

i.e., $2D + 4 \in L(a)$. By Lemma 2.3(2),

$$\Phi(L(a)) \leqslant \Phi(D+1, 2D, 2D+1, 2D+4) \leqslant D^2 - D.$$

Combining case 1 and case 2, Theorem 3.7 follows. ■

THEOREM 3.8. *Suppose $D \geqslant 6$ and $a \in M$. If $|L'(a)| = 2$, then*

$$\Phi(L(a)) \leqslant D^2 - D + 1.$$

Proof. Let $L'(a) = \{c_1, c_2\}$ and $B_0 = \{D + 1, c_1, c_2\}$. We consider $B_{D-4} = \{l_{D-4} + (D-4)K + j(D+1-K) : 0 \leqslant j \leqslant D-4\} \subset L(a)$, where K, l_{D-4}, and B_{D-4} are defined as in Definition 3.2.

If $B_0 (\text{mod } D+1) + B_{D-4} (\text{mod } D+1) = Z_{D+1}$, then by Lemma 2.2

$$\Phi(L(a)) \leqslant c_2 + l_{D-4} + (D-4)(D+1) - (D+1) + 1 \leqslant D^2 - D - 3.$$

Now we suppose $B_0(\text{mod } D+1) + B_{D-4}(\text{mod } D+1) \neq Z_{D+1}$. Since $\gcd(D+1, K) = 1$, then there exists some r such that $\gcd(D+1, r) = 1$ and $r(D+1-K) \equiv 1 \pmod{D+1}$. Let

$$B'_{D-4} = \{(b - l_{D-4} - (D-4)K)r \in Z_{D+1} : b \in B_{D-4}\}$$

$$= \{0, 1, \ldots, D-4\},$$

$$B'_0 = \{br \in Z_{D+1} : b \in B_0\} = \{0, c_1 r, c_2 r\}(\text{mod } D+1)$$

We can prove $B'_0 + B'_{D-4} \neq Z_{D+1}$. Noting that $|B'_{D-4}| \geqslant 3$, we can check that the only possible cases for $\{c_1 r, c_2 r\}$ modulo $D+1$ are the following:

$$\{c_1 r, c_2 r\} \subset \{1, 2, 3\} \quad \text{or} \quad \{c_1 r, c_2 r\} \subset \{-1, -2, -3\} \quad \text{or}$$

$$\{c_1 r, c_2 r\} \in \{\{1, -1\}, \{1, -2\}, \{-1, 2\}\}.$$

Case 1: $\{c_1 r, c_2 r\}(\text{mod } D+1) \subset \{1, 2, 3\}$ or $\{c_1 r, c_2 r\}(\text{mod } D+1) \subset \{-1, -2, -3\}$. We just prove the former; the latter can be proved similarly. It is easy to see that c_1, c_2 satisfy the conditions of Theorem 3.7, so $\Phi(L(a)) \leqslant D^2 - D$.

Case 2: $\{c_1 r, c_2 r\}(\text{mod } D+1) = \{1, -1\}(\text{mod } D+1)$. We can prove c_1, c_2 satisfy the conditions of Theorem 3.5, so $\Phi(D+1, c_1, c_2) \leqslant D^2 - D$.

Case 3: $\{c_1 r, c_2 r\}(\text{mod } D+1) = \{1, -2\}(\text{mod } D+1)$ or $\{-1, 2\}(\text{mod } D+1)$. We just prove the former; the latter can be proved similarly. It is easy to see that c_1, c_2 satisfy the conditions of Theorem 3.6, so $\Phi(D+1, c_1, c_2) \leqslant D^2 - D + 1$.

Combining cases 1 to 3, Theorem 3.8 follows. ■

MAIN THEOREM. *Suppose A is an $n \times n$ nonnegative and primitive matrix and D is the diameter of $D(A)$. Then*

$$\gamma(A) \leqslant D^2 + 1.$$

Proof. Without loss of generality, we suppose $D(A)$ satisfies hypothesis (*). It is sufficient for us to prove $a \xrightarrow{D^2+1} b$ for any $a, b \in V(D(A))$.

If $a \notin M$, then $a \xrightarrow{D^2-1} b$; by the arbitrariness of b we have $a \xrightarrow{D^2+1} b$.

If $a \in M$, then by Theorem 3.2, Theorem 3.3, Theorem 3.4, and Theorem 3.8, $a \xrightarrow{D^2+1} b$ is always true.

Therefore we have completed the proof of this conjecture. ■

I should like to thank Professor Qiao Li and Professor Jia-Yu Shao for their kind help and enthusiastic encouragement.

REFERENCES

1 R. E. Hartwig and Michael Neumann, Bounds on the exponent of primitivity which depend on the spectrum and the minimal polynomial, *Linear Algebra Appl.*, 184:103–122 (1993).

2 J. Shen, The proof of a conjecture about the exponent of primitive matrices, *Linear Algebra Appl.*, 216:185–203 (1995).

3 J. Shen, Some estimated formulas for the Frobenius numbers, *Linear Algebra Appl.*, to appear.

4 Y. Vitek, Bounds for a linear diophantine problem of Frobenius, *J. London Math. Soc.* 10:79–85 (1975).

5 J. B. Roberts, Notes on linear forms, *Proc. Amer. Math. Soc.* 7:456–469 (1956).

6 A. Brauer and B. M. Seflbinder, On a problem of partition II, *Amer. J. Math.* 76:343–346 (1954).

7 J. Y. Shao, On the exponent of a primitive digraph, *Linear Algebra Appl.* 64:21–31 (1985).

8 J. Y. Shao, Some formulas of the Frobenius numbers, *J. Math.* (*Wuhan*) 8:375–388 (1988).

9 R. E. Hartwig and X. D. Lin, The index of primitivity, Preprint, 1984.

10 J. H. B. Kemperman, On small sumsets in an Abelian group, *Acta Arith.* 103:63–88 (1960).

11 H. B. Mann, *Addition Theorems: The Addition Theorems of Group Theory and Number Theory*, Interscience.

12 Loo-king Hua, *An Introduction to Number Theory*, Science Press.

Received 11 July 1993; final manuscript accepted 7 September 1994