On Lewin and Vitek's Conjecture about the Exponent Set of Primitive Matrices

Zhang Ke Min
Department of Mathematics
Nanjing University
Nanjing, People's Republic of China

Submitted by Richard A. Brualdi

ABSTRACT

M. Lewin and Y. Vitek conjecture that every integer $\leqslant [\frac{1}{2}w_n] + 1 = [\frac{1}{2}(n^2 - 2n + 2)] + 1$ is the exponent of some $n \times n$ primitive matrix. In this paper we prove that this conjecture is true except for $n = 11$. The problem of determining the exponent set E_n is completely solved.

INTRODUCTION

An $n \times n$ nonnegative square matrix $A = (a_{ij})$ is primitive if $A^k > 0$ for some positive integer k. The least such k is called the exponent of A and is denoted by $\gamma(A)$.

1. THE MAIN RESULT

In 1950, H. Wielandt [6] first stated the exact general upper bound for $\gamma(A)$, that is, $\gamma(A) \leqslant W_n = (n-1)^2 + 1$ for all $n \times n$ primitive matrices. In 1964, A. L. Dulmage and N. S. Mendelsohn [1] revealed the so-called *gaps* in the exponent set of $n \times n$ primitive matrices. Each gap is a set S of consecutive integers below W_n such that no $n \times n$ matrix A has an exponent in S. In 1981, M. Lewin and Y. Vitek [4] found the general method for determining all gaps between $[\frac{1}{2}W_n] + 1$ and W_n, where $[x]$ denotes the greatest integer $\leqslant x$. And they conjectured that there are no gaps below

52 Vanderbilt Ave., New York, NY 10017 0024-3795/87/$3.50

$[\frac{1}{2}W_n]+1$. Recently, Shao Jia-Yu [5] proved that this conjecture is true for all sufficiently large n, but is not true for $n=11$. In this paper we prove that:

THEOREM. *Lewin and Vitek's conjecture is true except for* $n=11$. *Namely, there are no gaps below* $[\frac{1}{2}W_n]+1$ *except for* $n=11$.

By the proof of the Theorem, it is easy to show the following:

COROLLARY. *For* $n=11$, 48 *is the only number which does not satisfy Lewin and Vitek's conjecture.*

By the Theorem and [4], for any definite integer n, all the gaps in the exponent set of $n\times n$ primitive matrices are found. Then the problem of determining the exponent set is completely solved.

2. SOME KNOWN RESULTS ABOUT $\gamma(A)$

Let $r_1, r_2, \ldots, r_\lambda$ be a set of distinct positive integers with $(r_1, r_2, \ldots, r_\lambda)=1$. Then we define the Frobenius number $\phi(r_1, r_2, \ldots, r_\lambda)$ to be the least integer m such that every integer $k \geqslant m$ can be expressed in the form $k=a_1r_1+a_2r_2+\cdots+a_\lambda r_\lambda$, where $a_1, a_2, \ldots, a_\lambda$ are nonnegative integers. A result due to Schur shows that $\phi(r_1, r_2, \ldots, r_\lambda)$ is well defined if $(r_1, r_2, \ldots, r_\lambda)=1$. It is well known that

$$\phi(r_1, r_2)=(r_1-1)(r_2-1) \qquad \text{if} \quad (r_1, r_2)=1$$

and

$$\phi\big(n, n-1, \tfrac{1}{2}(n-1)\big)=\phi\big(n, \tfrac{1}{2}(n-1)\big)=(n-1)\big\{\tfrac{1}{2}(n-1)-1\big\}.$$

Let $E_n=\{m\in\mathbb{Z}^+ \mid m=\gamma(A)$ for some $n\times n$ primitive matrix $A\}$ and

$$\begin{aligned} E_n^{(1)} &= \big\{\big[\tfrac{1}{2}W_{n-1}\big]+2, \ldots, \big[\tfrac{1}{2}W_n\big]+1\big\} \\ &= \big\{\big[\tfrac{1}{2}(n^2-4n+9)\big], \ldots, \big[\tfrac{1}{2}(n^2-2n+4)\big]\big\}. \end{aligned}$$

Then we have some known results about $\gamma(A)$ as follows:

LEMMA 1 [5, §3, Lemma]. $E_1\subseteq E_2\subseteq\cdots\subseteq E_n\subseteq E_{n+1}\subseteq\cdots$.

LEMMA 2 [5, §7]. $48\in E_{11}^{(1)}$, $48\notin E_{11}$.

LEMMA 3 [5, Lemma 6.1 and Theorem 6.1].

(1) *Lewin and Vitek's conjecture is true for all* $n \leqslant 10$ *iff* $E_n^{(1)} \subseteq E_n$ $(n = 3,5,7,9)$ *is true.*

(2) *If* $\bigcup_{k=0}^{5} E_{2k+1}^{(1)} \subseteq E_{12}$, *then Lewin and Vitek's conjecture is true for all* $n \geqslant 12$ *iff* $E_n^{(1)} \subseteq E_n$ *is true for all odd numbers* $n \geqslant 12$.

LEMMA 4 [5, Theorem 4.1]. *If* $n \geqslant r_1 > r_2 > \cdots > r_\lambda$ *is a set of positive integers where* $(r_1, r_2, \ldots, r_\lambda) = 1$, *then*

$$\{\phi(r_1, r_2, \ldots, r_\lambda) + r_1 - 1, \ldots, \phi(r_1, r_2, \ldots, r_\lambda) + n + r_1 - r_2 - 1\} \subseteq E_n.$$

So Lewin and Vitek's conjecture is reduced to a number theoretical problem, that is, for odd integer n and any integer $m \in E_n^{(1)}$, to determine whether there are $r_1, r_2, \ldots, r_\lambda$ integers in Lemma 4 such that $m \in E_n$.

3. PROOF OF THE MAIN THEOREM

Before proving the Theorem, we need another lemma as follows: Let $p_1 = 3$, $p_2 = 7$, $p_3 = 11$, $p_4 = 19$, $p_5 = 23$, $p_6, \ldots, p_i, \ldots$ be the infinite sequence of all prime numbers of the form $4k + 3$, and denote $\mathscr{P}_3 = \{p_1, p_2, \ldots, p_i, \ldots\}$.

LEMMA 5. *If* $p_i, p_{i+1} \in \mathscr{P}_3$, *then* $p_{i+1} \leqslant 2p_i$, $i \geqslant 2$.

Proof. In [2, p. 491], Erdös proved that:

SATZ 9. *Für* $\xi \geqslant 6000$ *gibt es im intervall* $\xi < p \leqslant 2\xi$ *je eine primzahl von der form* $4k + 1$ *und* $4k + 3$.

Hence when $p_i \geqslant 6000$, we have $p_{i+1} \leqslant 2p_i$. On the other hand, when $p_i < 6000$, it is easy to check by the table of prime numbers in [3] that we have a sequence of the prime numbers of the form $4k + 3$ as follows:

$$7, 11, 19, 31, 59, 107, 211, 419, 827, 1627, 3251, 6491 \qquad \text{(A)}$$

For any $p_i < 6000$, there exist two consecutive numbers p and p' in (A) with $p \leqslant p_i < p'$, thus we have $p \leqslant p_i < p' \leqslant 2p \leqslant 2p_i$. Clearly $p_{i+1} \leqslant p'$. So $p_{i+1} \leqslant 2p_i$. This completes the proof of the lemma. ∎

LEMMA 6. *If $n \geqslant 43$ and $n \neq 50, 61, 72, 83, 94, 105$, then there exists a prime p (depending on n) satisfying the following properties:*

$$p \in \mathscr{P}_3, \tag{B1}$$

$$\tfrac{1}{4}(p-1)(p+3) \geqslant 19, \tag{B2}$$

$$\tfrac{1}{4}(p-1)(p+5) \leqslant n-3, \tag{B3}$$

$$n \not\equiv \tfrac{1}{2}(p+1) \pmod{p}. \tag{B4}$$

Proof. First, suppose $n \geqslant 273$. Let p_{h+1} be the least prime in $\mathscr{P}_3 \setminus \{3,7\}$ such that $n \not\equiv \frac{1}{2}(p_{h+1}+1) \pmod{p_{h+1}}$. Take $p = p_{h+1}$. Then (B1), (B2), (B4) follow easily from the choice of p. For (B3) we consider two cases:

Case 1: $h \leqslant 5$. In this case $p = p_{h+1} \leqslant p_6 = 31$. So $p+2 \leqslant 33 \leqslant \sqrt{4n-3}$. Hence (3) follows.

Case 2: $h > 5$. Note that $n \equiv \frac{1}{2}(p_h+1) \pmod{p_i}$ for all $i = 3,4,\ldots,h$, so

$$n \equiv \tfrac{1}{2}(p_3 p_4 \cdots p_h + 1) \pmod{p_i} \qquad \text{for all} \quad i = 3,4,\ldots,h.$$

But $p_3, p_4, \ldots, p_h$ are distinct primes, so

$$n \equiv \tfrac{1}{2}(p_3 p_4 \cdots p_h + 1) \pmod{p_3 p_4 \cdots p_h}$$

Hence $n \geqslant \frac{1}{2}(p_3 p_4 \cdots p_h + 1)$. Namely, $4n - 3 \geqslant 2p_3 p_4 \cdots p_h - 1$. On the other hand, for $h > 5$, by Lemma 5 we have

$$(p_{h+1}+2)^2 \leqslant 4p_{h+1}^2 \leqslant 32 p_h p_{h-1} \leqslant 2p_3 p_4 \cdots p_h - 1.$$

Hence we have $(p_{h+1}+2)^2 \leqslant 4n - 3$. So (3) follows.

If $43 \leqslant n < 273$, evidently, when $n \geqslant 43$ and $n \neq 11k+6$, we can take 11 instead of p of (B); when $n \geqslant 108$ and $n \neq 19k+10$, we can take 19 instead of p of (B). It is easy to check that for any n $(43 \leqslant n < 273)$ except for $50, 61, 72, 83, 94, 103$, there always exists one of $\{11, 19\}$ which satisfies (B). So the Lemma follows. ∎

LEMMA 7.

(1) *If n is odd $\geqslant 3$, then we have* $\{\frac{1}{2}(n^2-2n+1), \frac{1}{2}(n^2-2n+3)\} \subseteq E_n$.

(2) *If n is odd $\geqslant 5$, then we have* $\{\frac{1}{2}(n^2-4n+3), \ldots, \frac{1}{2}(n^2-3n+4)\} \subseteq E_n$.

Proof. (1): Let $\{r_1, r_2, r_3\} = \{n, n-1, \frac{1}{2}(n-1)\}$; thus $\phi(n, n-1, \frac{1}{2}(n-1)) = \frac{1}{2}(n^2 - 4n + 3)$. Hence we have $\{\frac{1}{2}(n^2 - 2n + 1), \frac{1}{2}(n^2 - 2n + 3)\} \subseteq E_n$ by Lemma 4.

(2): Let $\{r_1, r_2\} = \{n-2, \frac{1}{2}(n-1)\}$; thus we have $\{\frac{1}{2}(n^2 - 4n + 3), \ldots, \frac{1}{2}(n^2 - 3n + 4)\} \subseteq E_n$ by Lemma 4. ■

LEMMA 8. *If $n \geqslant 13$, then we have:*

(1) *If $n \equiv 1 \pmod 4$, then $E_n^{(1)} \subseteq E_n$ iff $\{\frac{1}{2}(n^2 - 2n - 3), \frac{1}{2}(n^2 - 2n - 1)\} \subseteq E_n$.*

(2) *If $n \equiv 3 \pmod 4$, then $E_n^{(1)} \subseteq E_n$ iff $\{\max[\frac{1}{2}(n^2 - 2n - 19), \frac{1}{2}(n^2 - 3n + 6)], \ldots, \frac{1}{2}(n^2 - 2n - 1)\} \subseteq E_n$.*

Proof. (1): $(\frac{1}{2}(n+1), n-3) = 1$, since $n \equiv 1 \pmod 4$. Let $r_1 = n - 3$ and $r_2 = \frac{1}{2}(n+1)$; then we have $\{\frac{1}{2}(n^2 - 3n - 4), \ldots, \frac{1}{2}(n^2 - 2n - 5)\} \subseteq E_n$ by Lemma 4. So (1) is true by Lemma 7.

(2): $(\frac{1}{2}(n+3), n-5) = 1$, since $n \equiv 3 \pmod 4$. Let $r_1 = n - 5$ and $r_2 = \frac{1}{2}(n-3)$; then we have $\{\frac{1}{2}(n^2 - 3n - 18), \ldots, \frac{1}{2}(n^2 - 2n - 21)\} \subseteq E_n$ by Lemma 4. So (2) is true by Lemma 7. ■

LEMMA 9. *If n is odd, $n \geqslant 43$, and $n \neq 61, 83, 105$, then we have $E_n^{(1)} \subseteq E_n$.*

Proof. Let $r_1 = n - \frac{1}{2}(p+1)$ and $r_2 = \frac{1}{2}[n + \frac{1}{2}(p-1)]$, where p is the prime number satisfying the properties (B) in Lemma 6. By (B1), $p \equiv 3 \pmod 4$, so r_2 is an integer, since n is odd. By (B3), $p < \frac{1}{3}(2n-1)$, so $r_1 > r_2$. Also we have that either $(r_1, r_2) = p$ or $(r_1, r_2) = 1$, since $2r_2 - r_1 = p$. But if $(r_1, r_2) = p$, then $r_1 = n - \frac{1}{2}(p+1) \equiv 0 \pmod p$. So $n \equiv \frac{1}{2}(p+1) \pmod p$; this contradicts (B4). Hence $(r_1, r_2) = 1$. Now we use Lemma 4 to get

$$\phi(r_1, r_2) + r_1 - 1 = \tfrac{1}{2}\{n^2 - 2n - \tfrac{1}{4}(p-1)(p+3)\} \leqslant \tfrac{1}{2}(n^2 - 2n - 19)$$

by (B2);

$$\phi(r_1, r_2) + n + r_1 - r_2 - 1 = \tfrac{1}{2}\{n^2 - 2n + 3 + [n - 3 - \tfrac{1}{4}(p-1)(p+5)]\}$$

$$\geqslant \tfrac{1}{2}(n^2 - 2n + 3)$$

by (B3). And

$$\left\{\tfrac{1}{2}(n^2-2n-19),\ldots,\tfrac{1}{2}(n^2-2n+3)\right\}\subseteq E_n.$$

Hence we get the lemma by Lemma 8. ■

LEMMA 10. *If* $n=2k+1$ $(k=1,2,\ldots,20),61,83,105$, *then* $E_n^{(1)}\subseteq E_n$ *if* $n\neq 11$; *and* $E_{11}^{(1)}\setminus\{48\}\subseteq E_{11}$.

Proof. We divide the proof into five steps:

(1) By Lemmas 7 and 8, for proving this Lemma, it is enough to prove that

$$E_n^{(2)}\subseteq E_n,$$

where $E_n^{(2)}$ is as shown in Table 1.

(2) Let $r_1=n-2$, $r_2=\frac{1}{2}(n+1)$. If $n\not\equiv 5 \pmod 6$ and $n=2k+1\geqslant 7$, then $(r_1,r_2)=1$. Since $(r_1-1)r_2=\frac{1}{2}(n^2-2n-3)$ and $(r_1-2)r_2+n=\frac{1}{2}(n^2-n-4)$, we have $\{\frac{1}{2}(n^2-2n-3),\ \frac{1}{2}(n^2-2n-1)\}\subseteq E_n$ by Lemma 4. Also, for proving $E_n^{(2)}\subseteq E_n$, it is enough to prove that $E_n^{(3)}\subseteq E_n$, where $E_n^{(3)}$

TABLE 1

n	$E_n^{(2)}$	n	$E_n^{(2)}$
7	17	29	390,391
9	30,31	31	440,441,...,449
11	47,49	33	510,511
13	70,71	35	568,569,...,577
15	93,94,...,97	37	646,647
17	126,127	39	712,713,...,721
19	155,156,...,161	41	798,799
21	198,199	61	1798,1799
23	233,234,...,241	83	3352,3353,...,3361
25	286,287	105	5406,5407
27	328,329,...,337		

is as follows:

n	$E_n^{(3)}$	n	$E_n^{(3)}$
11	47,49	29	390,391
15	93,94,95	31	440,441,...,447
17	126,127	35	568,569,...,577
19	155,156,...,159	39	712,713,...,719
23	233,234,...,241	41	798,799
27	328,329,...,335	83	3352,3353,...,3361

(3) Let $r_1 = n-4$, $r_2 = \frac{1}{2}(n+3)$. If $n \not\equiv 11 \pmod{14}$ and $n = 2k+1 \geqslant 13$, then $(r_1, r_2) = 1$. Since $(r_1-1)r_2 = \frac{1}{2}(n^2-2n-15)$ and $(r_1-2)r_2 + n = \frac{1}{2}(n^2-n-18)$, we have $\{\frac{1}{2}(n^2-2n-15),\ldots,\frac{1}{2}(n^2-n-18)\} \subseteq E_n$ by Lemma 4. Also, for proving $E_n^{(3)} \subseteq E_n$, it is enough to prove that $E_n^{(4)} \subseteq E_n$, where $E_n^{(4)}$ is as follows:

n	$E_n^{(4)}$	n	$E_n^{(4)}$
11	47,49	35	568,569
23	233	39	712,713,...,719
27	328,329	83	3352,3353
31	440,441		

(4) Let $r_1 = n-6$, $r_2 = \frac{1}{2}(n+5)$. If $n \not\equiv 17 \pmod{22}$ and $n = 2k+1 \geqslant 19$, then $(r_1, r_2) = 1$. Since $(r_1-1)r_2 = \frac{1}{2}(n^2-2n-35)$ and $(r_1-2)r_2 + n = \frac{1}{2}(n^2-n-40)$, we have $\{\frac{1}{2}(n^2-2n-35),\ldots,\frac{1}{2}(n^2-n-40)\} \subseteq E_n$ by Lemma 4. Also, for proving $E_n^{(4)} \subseteq E_n$, it is enough to prove that $E_n^{(5)} \subseteq E_n$, where $E_n^{(5)}$ is as follows:

n	$E_n^{(5)}$	n	$E_n^{(5)}$
11	47,49	83	3352,3353
39	712,713,...,719		

(5) For convenience, we use the symbol $(n; r_1, r_2; (r_1-1)r_2, (r_1-2)r_2 + n)$. From (11; 11, 4; 40, 47), (11; 8, 7; 49, 49), (39; 29, 25; 700, 714), (39; 32, 23; 713, 729), and (83; 72, 47; 3352, 3361), we have $E_n^{(5)} \subseteq E_n$ by Lemma 4. This completes the proof of the lemma. ■

Now, we are ready to prove the Theorem.

Proof of the Theorem. From (12; 11, 4; 40, 48) we have $48 \in E_{12}$. Hence $\bigcup_{k=0}^{5} E_{2k+1}^{(1)} \subseteq E_{12}$ by Lemmas 1, 3(1), and 10. Therefore by Lemmas 2, 3, 9, and 10, the proof of the main Theorem is completed. ■

REFERENCES

1 A. L. Dulmage and N. S. Mendelsohn, Gaps in the exponent set of primitive matrices, *Illinois J. Math.* 8:642–656 (1964).
2 P. Erdös, Über die primzahlen gewisser arithmetischer reihen, *Math. Z.* 39:473–491 (1935).
3 D. N. Lehmer, *List of Prime Numbers from 1 to 10,006,721*, Carnegie Inst. Washington, 1914.
4 M. Lewin and Y. Vitek, A system of gaps in the exponent set of primitive matrices, *Illinois J. Math.* 25(1):87–98 (Spring 1981).
5 Shao Jia-Yu, On a conjecture about the exponent set of primitive matrices, *Linear Algebra Appl.* 65:91–123 (1985).
6 H. Wielandt, Unzerlegbare, nicht negative matrizen, *Math. Z.* 52:642–648 (1950).

Received 18 August 1986; revised 12 December 1986