THE EXPONENTS OF STRONGLY CONNECTED GRAPHS

EDWARD A. BENDER AND THOMAS W. TUCKER

1. Introduction. A *directed graph* G is a set of *vertices* V and a subset of $V \times V$ called the *edges* of G. A *path* in G of length k,

$$[v_1, v_2, \ldots, v_k, v_{k+1}],$$

is such that (v_i, v_{i+1}) is an edge of G for $1 \leqq i \leqq k$. A directed graph G is *strongly connected* if there is a path from every vertex of G to every other vertex. A *circuit* is a path whose two end vertices are equal. An *elementary circuit* has no other equal vertices. See (**1**) for a fuller discussion.

Let G be a finite, strongly connected, directed graph (fscdg). The kth *power* G^k of G is the directed graph with the same vertices as G and edges of the form (i, j), where G has a path of length k from i to j. It is easily shown (**6**) that we can define the *period* $p(G)$ and *exponent* $\gamma(G)$ as follows:

(i) p is the least positive integer such that for all sufficiently large t,

$$G^t = G^{t+p}, \tag{1}$$

(ii) γ is the least positive integer such that (1) holds whenever $t \geqq \gamma$.

The *exponent set* $\Gamma(n, p)$ is the set of all exponents of all n-vertex fscdgs with period p.

There is some information on $\Gamma(n, p)$ in the literature. Heap and Lynn (**4**) have shown:

$$\max \Gamma(n, p) \leqq p\left(\left[\frac{n}{p}\right] - 1\right)\left(\left[\frac{n}{p}\right] - 2\right) + 2n - p\left[\frac{n}{p}\right], \tag{2}$$

where [ ] denotes the greatest integer function. Wielandt (**9**) observed that

$$\max \Gamma(n, 1) = (n-1)(n-2) + n. \tag{3}$$

Dulmage and Mendelsohn (**3**) showed the existence of *gaps* in $\Gamma(n, 1)$ for $n \geqq 4$: if n is even and

$$n^2 - 4n + 6 < x < (n-1)^2 \tag{4}$$

or n is odd and

$$n^2 - 4n + 6 < n^2 - 3n + 2 \quad \text{or} \quad n^2 - 3n + 4 < x < (n-1)^2, \tag{5}$$

then $x \notin \Gamma(n, 1)$. They also showed that any other integer x satisfying $(n-2)^2 \leqq x \leqq (n-1)^2 + 1$ is in $\Gamma(n, 1)$.

Received July 7, 1967. Part of the paper is contained in the second author's senior thesis (**8**).

We will investigate $\Gamma(n, p)$ in detail. A simple algorithm will be given for determining $\Gamma(n, 1)$ for large enough n. It has been used to find $\Gamma(n, 1)$ for $35 \leqq n \leqq 100$ (in less than one minute!) on an IBM 7094. Inequality (2) will be replaced by a generalization of (3). Gaps will be established in $\Gamma(n, p)$ for all sufficiently large n. In fact, if

$$k \leqq x \leqq l \text{ implies } x \notin \Gamma\left(\left[\frac{n}{p}\right], 1\right),$$

then

$$pk \leqq y \leqq pl \text{ implies } y \notin \Gamma(n, p).$$

2. Computing exponents. Let G be an fscdg with elementary circuit lengths p_α, $1 \leqq \alpha \leqq e$. It is known (**6**) that

$$p(G) = \gcd(p_\alpha). \tag{6}$$

If l_1 and l_2 are the lengths of two paths from i to j in G, we have

$$l_1 \equiv l_2 \pmod{p(G)}$$

since there is a path from j to i of length l_3 and

$$l_1 + l_3 \equiv 0 \equiv l_2 + l_3 \pmod{p(G)}.$$

The *reach* from i to j, written h_{ij}, is the least non-negative integer such that there is a path from i to j of length

$$h_{ij} + lp \quad \text{for all } l \geqq 0.$$

(We allow paths of length 0 from i to i.) The following theorem is found in (**3**) for $p = 1$ and implicitly in (**4**).

THEOREM 2.1. *If G is an fscdg, then*

$$\gamma(G) = \max_{i,j \in V(G)} h_{ij} - p(G) + 1, \tag{7}$$

where $V(G)$ is the set of vertices of G.

Proof. Let $h_{kl} = \max h_{ij}$. There is no path of length $h_{kl} - p(G)$ from k to l. Hence, $\gamma(G) \geqq \max h_{ij} - p + 1$. On the other hand, let there be a path of length l from i to j and let $t \geqq h_{ij} - p + 1$ satisfy $t \equiv l \pmod{p}$. Then $h_{ij} \equiv l \equiv t \pmod{p}$. Hence, $t \geqq h_{ij}$. Thus, there is a path of length t from i to j, hence, $\gamma(G) \leqq \max h_{ij} - p + 1$.

Let r_{ij} be the length of the shortest path from i to j which contains a point of a circuit of every circuit length occurring in G (r_{ii} may be 0). We say that $(i; j)$ has the *unique path property* (upp) if, whenever $l > r_{ij}$ is the length of a path from i to j,

$$l = r_{ij} + \sum k_\alpha p_\alpha, \qquad k_\alpha \geqq 0. \tag{8}$$

https://doi.org/10.4153/CJM-1969-088-3 Published online by Cambridge University Press

The *Frobenius function* $F(l_1, l_2, \ldots, l_s)$ is the greatest multiple of $\gcd(l_\alpha)$ which is *not* expressible in the form

$$\sum k_\alpha l_\alpha, \qquad k_\alpha \geqq 0.$$

By a lemma of Schur (**2**), the function is not infinite.

For $p = 1$ in the following theorem, see (**3**).

THEOREM 2.2. *Let G be an fscdg with elementary circuit lengths p_α, $1 \leqq \alpha \leqq e$. If $i, j \in V(G)$, then*

$$h_{ij} \leqq r_{ij} + F(p_1, \ldots, p_e) + p(G), \tag{9}$$

with equality if $(i;j)$ has the upp and either no $p_\alpha = p(G)$ or no path from i to j has length $r_{ij} - p(G)$.

Proof. There is a path of length l from i to j for any l of the form (8). The inequality follows from (6) and the definition of F. Let $(i;j)$ have the upp. If some $p_\alpha = p$, then $r_{ij} + F = r_{ij} - p$. If no $p_\alpha = p$, then $F > 0$ and by the definitions of F and r_{ij}, there is no path of length $r_{ij} + F$ from i to j.

It can be shown (**6**) that G^p is the union of p disjoint fscdgs $G_1, \ldots, G_p$. The edges of G connect elements of $V(G_i)$ to elements of $V(G_{i+1})$, the subscript being understood modulo p. It follows that the elementary circuits of G_i have lengths p_α/p, $1 \leqq \alpha \leqq c$. By (6) we have $p(G_i) = 1$. The relationship between $\gamma(G)$ and $\gamma(G_i)$ is more complicated.

THEOREM 2.3. *Let G be an fscdg with $p = p(G) > 1$ and let S be a non-empty subset of $\{1, 2, \ldots, p\}$. Then*

$$p \max_{1\leqq i\leqq p} \gamma(G_i) - p + 1 \leqq \gamma(G) \leqq p \max_{s\in S} \gamma(G_s) + p - |S|, \tag{10}$$

where $|S|$ is the cardinality of S and G^p is the union of the disjoint fscdgs $G_1, \ldots, G_p$.

Proof. We establish the left-hand inequality first. Let $\gamma(G_k) = \max \gamma(G_i)$. By applying (7) to G_k, it follows that there are $i, j \in V(G_k)$ with $h_{ij} = \gamma(G_k)$, where the reach is in G_k. The corresponding reach in G is $p\gamma(G_k)$. Applying (7) to G proves the left-hand side of (10). Now let $i, j \in V(G)$. It suffices to show that

$$h_{ij} \leqq p \max_{s\in S} \gamma(G_s) + 2p - |S| - 1$$

and then apply (7). Starting at i on any path we reach some $k \in V(G_s)$ for some $s \in S$, and this path has length at most $p - |S|$. Working backwards from j, we see that there is a path of length at most $p - 1$ from some $l \in V(G_s)$ to j. For every $t \geqq \gamma(G_s)$ there is a path from k to l of length t in G_s since $p(G_s) = 1$. Combining these three paths (taking the one from k to l in G gives it length pt) yields the desired result.

COROLLARY 2.4. $\max_{1 \leqq i \leqq p} \gamma(G_i) - \min_{1 \leqq i \leqq p} \gamma(G_i) \leqq 1$.

Proof. Let $S = \{s\}$, where $\gamma(G_s) = \min \gamma(G_i)$.

The following theorem is proved in (**3**) for $p = 1$.

THEOREM 2.5. *If G is an fscdg with $p = p(G)$ and with s equal to the length of the shortest circuit of G, then*

$$\gamma(G) \leqq n + s\left(\left[\frac{n}{p}\right] - 2\right). \tag{11}$$

Proof. We assume the case $p = 1$; see (**3**, Theorem 1). Let

$$S^- = \left\{i\colon |V(G_i)| < \left[\frac{n}{p}\right]\right\}, \qquad S^0 = \left\{i\colon |V(G_i)| = \left[\frac{n}{p}\right]\right\}.$$

If $S^- \neq \emptyset$, let $S = S^-$ in (10). By applying the case $p = 1$ to G_i, where $i \in S$, we have:

$$\gamma(G) \leqq p\left(\left[\frac{n}{p}\right] - 1 + \frac{s}{p}\left(\left[\frac{n}{p}\right] - 3\right)\right) + p - |S^-| < n + s\left(\left[\frac{n}{p}\right] - 2\right).$$

If $S^- = \emptyset$; then

$$|S^0| \geqq p - \left(n - p\left[\frac{n}{p}\right]\right).$$

Apply (10) with $S = S^0$.

In the next section it will be shown that the bound in (11) is sharp whenever $[n/p]$ and s/p are relatively prime.

3. Some elements of $\Gamma(n, p)$.

The following observation is quite useful.

THEOREM 3.1. $\Gamma(n, p) \subseteq \Gamma(n + 1, p)$.

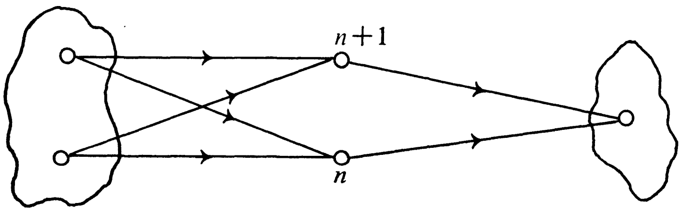
Proof. Let G be a given n-vertex fscdg. We shall construct an $(n + 1)$-vertex fscdg G' with $p(G') = p(G)$ and $\gamma(G') = \gamma(G)$. Let $V(G) = \{1, 2, \ldots, n\}$ and $V(G') = \{1, 2, \ldots, n + 1\}$. Let (i, j) be an edge of G' if and only if after replacing any $(n + 1)$'s by n's we obtain an edge of G; see Figure I. It is easily seen that $p(G') = p(G)$ and that the reach from i to j in G' is the same as the corresponding reach in G ($(n + 1)$'s replaced by n's). By (7) we have $\gamma(G') = \gamma(G)$.

LEMMA 3.2. *Let $m > s > 0$ and let l satisfy $s - m \leqq l \leqq s - 1$. Define $p = \gcd(m, s)$ and $n = \max(m, m + l)$. Then*

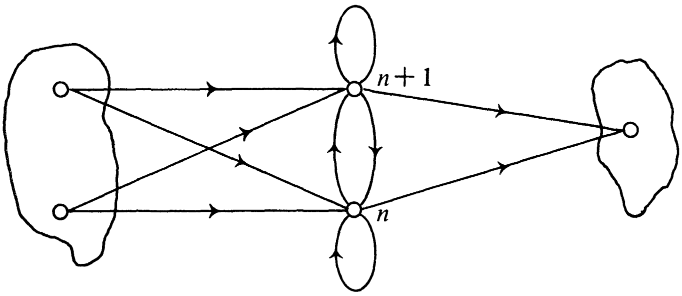
$$(m/p - 1)s + (m - s) + l \in \Gamma(n, p). \tag{12}$$

Proof. We explicitly construct a graph $G(m, s, l)$. Let $V(G) = \{1, 2, \ldots, n\}$; see Figure II.

https://doi.org/10.4153/CJM-1969-088-3 Published online by Cambridge University Press

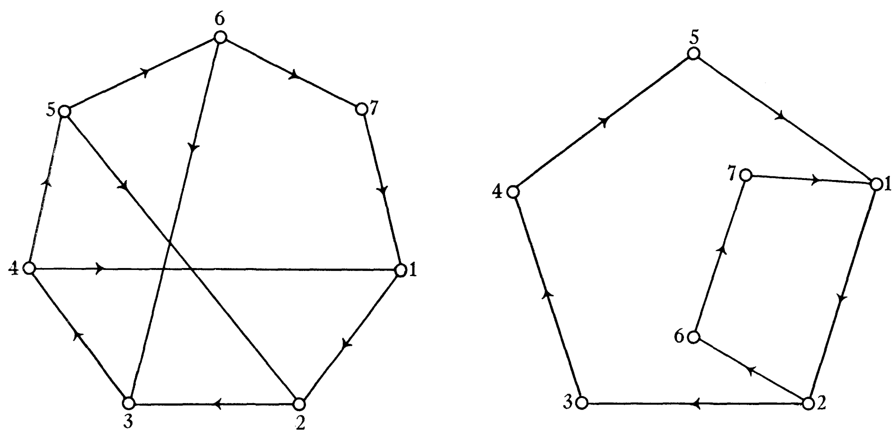


no loop at n



a loop at n

FIGURE I. *The graph* G'



$G(7, 4, -2)$ $G(5, 4, 2)$

FIGURE II. $G(m, s, l)$

Case I. $l \leqq 0$. Then $n = m$. Let the edges of $G(m, s, l)$ be

$$(i, i+1), \qquad 1 \leqq i \leqq n,$$
$$(s+k-1, k), \qquad 1 \leqq k \leqq 1-l,$$

where we agree to identify 1 and $n+1$.

https://doi.org/10.4153/CJM-1969-088-3 Published online by Cambridge University Press

Case II. $l > 0$. Let the edges of $G(m, s, l)$ be

$$\begin{array}{ll} (i, i+1), & 1 \leqq i < m, \\ (m, 1), & \\ (s-l, m+1), & \\ (m+k, m+k+1) & 1 \leqq k \leqq l. \end{array}$$

It is easily seen that $(s - l + 1; m)$ has the upp and $r_{ij} \leqq r_{s-l+1,m}$ for all vertices i, j. By Theorems 2.1 and 2.2 and the well-known (**2**) formula $F(m, s) = ms/p - m - s$, we have:

$$\begin{aligned} \gamma(G(m, s, l)) &= r_{s-l+1,m} + F(m, s) + 1 \\ &= 2m - (s - l + 1) + \frac{ms}{p} - m - s + 1 \\ &= \left(\frac{m}{p} - 1\right)s + (m - s) + l. \end{aligned}$$

By taking $m = p[n/p]$ and $l = n - m$ in (12), we see that (11) is sharp when $[n/p]$ and s/p are relatively prime. In particular, (2) may be replaced by the following generalization of (3).

THEOREM 3.3. *If* $n \geqq 2p$, *then*

$$\max \Gamma(n, p) = p\left(\left[\frac{n}{p}\right] - 1\right)\left(\left[\frac{n}{p}\right] - 2\right) + n. \tag{13}$$

Proof. Since $n \geqq 2p$, we have $s \leqq p([n/p] - 1)$ in (11).

Let $g(n, p)$ be the least positive integer *not* in $\Gamma(n, p)$; that is, the start of the first gap. Results like the following have been obtained by Dulmage, Mendelsohn, and Norman (**5**).

THEOREM 3.4. $g(n, p) \geqq p[(n + 2p + 1)/2p]^2 - 2p$.

Proof. By Theorem 3.1 and (12) with $m = p(k - 1)$ and $s = p(k - 2)$ and $-p \leqq l \leqq p(k - 3) - 1$ we have for $k \geqq 3$:

(i) $x \in \Gamma(p(2k - 4) - 1, p)$ for $p(k - 2)^2 \leqq x \leqq p(k^2 - 3k + 2) - 1$.

If $k > 3$ is even, let $m = p(k + 1)$, $s = p(k - 3)$. By Theorem 3.1 and (12),

(ii) $x \in \Gamma(p(2k - 2) - 1, p)$ for $p(k^2 - 3k) \leqq x \leqq p(k - 1)^2 - 1$,

(ii′) $x \in \Gamma(p(2k - 4) - 1, p)$ for $p(k^2 - 3k) \leqq x \leqq p(k^2 - 2k - 1) - 1$.

If $k \geqq 3$ is odd, we take $m = pk$ and $s = p(k - 2)$ to obtain

(iii) $x \in \Gamma(p(2k - 3) - 1, p)$ for $p(k^2 - 3k + 2) \leqq x \leqq p(k - 1)^2 - 1$,

(iii′) $x \in \Gamma(p(2k - 4) - 1, p)$ for $p(k^2 - 3k + 2) \leqq x \leqq p(k^2 - 2k) - 1$.

Apply Theorem 3.1 using (i)–(iii′) as follows:

(i): $3 \leqq k \leqq l + 1$,
(ii), (iii): $3 \leqq k \leqq l$, depending on the parity of k,
(ii′), (iii′): $k = l + 1$, depending on the parity of k.

This yields:

$$\text{(iv)} \qquad x \in \Gamma(p(2l-2)-1, p) \quad \text{for } p \leqq x \leqq p(l^2-2).$$

With $m = s = p$ in Case II of the proof of Lemma 3.2 and $(s - l + 1; m)$ replaced by $(m + 1; m)$, the range of x in (iv) can be extended down to 1. We have:

$$g(p(2l-2)-1, p) \geqq p(l^2-2).$$

Let

$$l = \left[\frac{n+2p+1}{2p}\right]$$

and use the fact that g is monotonic.

Theorem 3.4 and (13) show that $g(n, p) > \max \Gamma(n, p)/4$ for $n \geqq 3p$. When n is large, much more is true.

THEOREM 3.5. *For fixed* p,

$$(14) \qquad g(n, p) \sim \frac{n^2}{p} \sim \max \Gamma(n, p).$$

Proof. By Theorems 3.1, 3.3, and 3.4, it suffices to show that for every $\epsilon > 0$ and sufficiently large k:

$$\text{if } p(k-2)^2 \leqq x \leqq p(k-1)^2, \quad \text{then } x \in \Gamma(p(k-1)(1+\epsilon), p).$$

Assume that $0 < \delta < 1$, we shall choose it later. Let k be so large that there are at least two primes between $2y + 1$ and $2(1 + \delta)y + 1$ whenever $y \geqq (2k - 1)^{1/2}$ (this is possible by the prime number theorem). For x as above, let $y = (k^2 - x/p)^{1/2}$. One of the two guaranteed primes is prime to $2k + 1$ since $(2y + 1)^2 > 2k + 1$. Call it $2j + 1$. Let

$$m = p(k+j+1), \qquad s = p(k-j).$$

Then

$$\begin{aligned}
\gcd\left(\frac{m}{p}, \frac{s}{p}\right) &= \gcd(k+j+1, k-j) \\
&= \gcd(k+j+1+k-j, k+j+1-(k-j)) \\
&= \gcd(2k+1, 2j+1) \\
&= 1,
\end{aligned}$$

$$\left(\frac{m}{p} - 1\right)s = p(k^2 - j^2) \leqq x,$$

$$\begin{aligned}
p(k^2-j^2) &\geqq pk^2 - p(1+\delta)^2\left(k^2 - \frac{x}{p}\right) \\
&> x - 3\delta p\left(k^2 - \frac{x}{p}\right) \\
&\geqq x - 12\delta p(k-1).
\end{aligned}$$

Hence, we may choose $0 \leqq l < 12\delta p(k-1)$ in (12) so that we have $x \in \Gamma(n, p)$. Now

$$\begin{aligned} n &= m + l \\ &< p(k + j + 1) + 12\delta p(k-1) \\ &< p(k + 1 + 8(k-1)^{1/2} + 12\delta(k-1)). \end{aligned}$$

Choose k so large and δ so small that

$$\epsilon \geqq \frac{2}{k-1} + \frac{8}{(k-1)^{1/2}} + 12\delta$$

and

$$p(k-j) \geqq 12\delta p(k-1).$$

4. The gaps of $\Gamma(n, p)$. The gaps in $\Gamma(n, 1)$ above $(n-2)^2$ were already mentioned in (4) and (5). When $n \geqq 8$, this result is a special case of the following theorem.

THEOREM 4.1. *If $x > \frac{1}{2}n(n+1)$, then $x \in \Gamma(n, 1)$ if and only if*

$$x = (m-1)s + m - s + l$$

for some integers m, s, l such that

$$\gcd(m, s) = 1, \qquad n \geqq m > s > 0,$$
$$s - 1 \geqq l \geqq s - m, \qquad n \geqq m + l.$$

Proof. The sufficiency follows from Theorem 3.1 and (12). We shall prove the necessity in this section.

Combining this result with (14), we see that a relatively easy method exists for determining $\Gamma(n, 1)$ for sufficiently large n. The values of $g(n, 1)$ given in Table I indicate that $n \geqq 35$ may be "sufficiently large".

TABLE I

Values of $g(n, 1)$

	0	1	2	3	4	5	6	7	8	9
20	231	232	233?	284	285?	349	350?	453	454	472
30	473	474?	585	586	587?	686	687	774	914	915
40	916	917	1099	1175	1235	1317	1359	1424	1425	1535
50	1691	1692	1718	1867	1947	1994	1995	1996	2131	2316
60	2317	2318	2319	2665	2697	2933	2934	2935	2936	3262
70	3321	3322	3323	3625	3626	3802	3803	4011	4055	4269
80	4656	4779	4803	4804	4805	4817	4818	5058	5059	5060
90	5061	5062	5793	5794	5795	6202	6594	6595	6596	6599
100	7073									

At present, no comparable result is known for $\Gamma(n, p)$ with $p > 1$. However, the existence of numerous gaps in $\Gamma(n, p)$ can be established.

THEOREM 4.2. *If* $x \notin \Gamma([n/p], 1)$ *for* $k \leqq x \leqq l$, *then*

$$y \notin \Gamma(n, p) \quad \text{for } pk \leqq y \leqq pl; \tag{15}$$

if in addition $k - 1 \notin \Gamma([n/p] - 1, 1)$, *then*

$$y \notin \Gamma(n, p) \quad \text{for } p(k-1) + w + 1 \leqq y \leqq pl, \tag{16}$$

where $w = n - p[n/p]$.

Proof. Let $\gamma(G) = y \in \Gamma(n, p)$ and $y \leqq pl$. By (10) we have

$$\gamma(G_i) \leqq l + (p-1)/p$$

for all i. Since $\gamma(G_i)$ is an integer, $\gamma(G_i) \leqq l$. We now use the given gap data. Let

$$S^- = \left\{i: |V(G_i)| < \left[\frac{n}{p}\right]\right\}, \qquad S^0 = \left\{i: |V(G_i)| = \left[\frac{n}{p}\right]\right\}.$$

If $S^- \neq \emptyset$, let $S = S^-$ in (10). Then

$$\gamma(G) \leqq pk' + p - |S^-| \leqq p(k'+1) - 1,$$

where $k' < k$ in (15) and $k' < k - 1$ in (16). If $S^- = \emptyset$, let $S = S^0$. We have:

$$\begin{aligned}\gamma(G) &\leqq pk' + p - |S^0| \\ &\leqq p(k-1) + p - \left(p - n + p\left[\frac{n}{p}\right]\right) \\ &\leqq p(k-1) + w.\end{aligned}$$

Study of some special cases has shown that $y \leqq pl$ in (15) is not best possible (hence, a similar conclusion holds for the left half of (10)). It is not known what is best possible, however $y \leqq pl + p - 1$ seems likely when (4) and (5) are used for $\Gamma([n/p], 1)$.

We devote the remainder of this paper to developing the machinery needed for proving Theorem 4.1.

THEOREM 4.3. *Let* $0 < p_1 < \ldots < p_e$ *be given with* $e \geqq 3$. *Then*

$$F(p_1, \ldots, p_e) < \frac{p_e^2}{2\gcd(p_\alpha)} - p_e.$$

Proof. If $\gcd(p_\alpha) = d$, we have

$$F(p_1, \ldots, p_e) = dF(p_1/d, \ldots, p_e/d).$$

It suffices to consider $d = 1$. If $p_e \geqq 2p_1$, then (**2**)

$$F(p_1, \ldots, p_e) \leqq p_1p_e - p_1 - p_e \leqq \tfrac{1}{2}p_e(p_e - 3).$$

https://doi.org/10.4153/CJM-1969-088-3 Published online by Cambridge University Press

Suppose that there exists a, possibly reordered, subsequence of p_α, say q_β, $1 \leqq \beta \leqq k$, such that

$$k \geqq 3,$$
$$d_\beta > d_{\beta+1}, \text{ where } d_\beta = \gcd(d_{\beta-1}, q_\beta) \text{ and } d_1 = q_1,$$
$$d_k = 1.$$

Then (2)

$$F(p_1, \ldots, p_e) \leqq F(q_1, \ldots, q_k) \leqq \sum_{\beta=1}^{k-1} \frac{d_\beta}{d_{\beta+1}} q_{\beta+1} - \sum_{\beta=1}^{k} q_\beta.$$

The maximum occurs when all $d_\beta/d_{\beta+1}$ are minimal except one. Let

$$Q = \max q_\beta \qquad (\beta \neq 1).$$

Since $d_{\beta+1}$ is a proper divisor of d_β,

$$\begin{aligned} F(p_1, \ldots, p_e) &\leqq Q \sum_{\beta=1}^{k-1} \left(\frac{d_\beta}{d_{\beta+1}} - 1\right) - q_1 \\ &\leqq Q\left((k-3) + \frac{q_1}{2^{k-2}}\right) - q_1 \\ &\leqq Q\frac{q_1}{2} - q_1 \quad \text{since } k \geqq 3 \text{ and } q_1 \geqq 2^{k-2} \\ &\leqq \tfrac{1}{2}(p_e - 1)(p_e - 2) \quad \text{since } Q \neq q_1. \end{aligned}$$

Suppose that three p_α's, say $a, a - d, a - 2d$, are relatively prime and form an arithmetic progression. Then (7)

$$\begin{aligned} F(p_1, \ldots, p_e) &\leqq F(a, a - d, a - 2d) \\ &= (\tfrac{1}{2}(a - 2d - 2) + 1)(a - 2d) + (d - 1)(a - 2d - 1) - 1 \\ &\leqq \tfrac{1}{2}(a - 2d)(a - 2) - d \\ &\leqq \tfrac{1}{2}(a - 2)^2 - 1 \\ &< \tfrac{1}{2}(p_e - 2)^2. \end{aligned}$$

In the above situation we have shown that

$$F < \tfrac{1}{2}p_e(p_e - 2).$$

This will be called Case I in the proof of the corollary. Case II is the situation in which $c > b > a$ are three p_α's which are pairwise prime, not in an arithmetic progression, and satisfy $2a > c$. Define c^* by

$$c^*c \equiv a \pmod b, \qquad |c^*| < \tfrac{1}{2}b$$
(possible since $b > 2$ and c^* is prime to b).

Assume that

$$M \geqq a\left[\frac{b}{|c^*|}\right] + c(|c^*| - 1) = M_0.$$

https://doi.org/10.4153/CJM-1969-088-3 Published online by Cambridge University Press

We will show that M is a non-negative linear combination of a, b, and c so that $F(a, b, c) < M_0$. Let λ and μ be integers with $\lambda a + \mu b = M$. It suffices to construct integers x, y, and w with

$$(*) \qquad ya - wb \geqq 0, \qquad xb - yc \geqq -\lambda, \qquad wc - xa \geqq -\mu,$$

since $M = (xb - yc + \lambda)a + (wc - xa + \mu)b + (ya - wb)c$. Let ϵ and η be defined by

$$c\,\eta \equiv \epsilon \pmod{b}, \qquad 0 \leqq \epsilon \leqq |c^*| - 1, \quad \lambda - \left[\frac{b}{|c^*|}\right] \leqq \eta \leqq \lambda.$$

Let x, y, and w satisfy

$$bx \equiv -\eta \pmod{c}, \quad y = \left[\frac{bx + \lambda}{c}\right] \geqq \frac{bx + \eta}{c}, \quad w = \left[\frac{ay}{b}\right].$$

Clearly, the first two inequalities in (*) hold. We have:

$$a\left(\frac{bx + \eta}{c}\right) \equiv cc^*\left(\frac{bx + \eta}{c}\right) \pmod{b} \equiv c^*\eta \equiv \epsilon.$$

Hence

$$w \geqq \frac{a(c^{-1}(bx + \eta)) - \epsilon}{b} = \frac{abx + a\eta - ce}{bc}.$$

Thus,

$$\begin{aligned} wc - xa &\geqq \frac{abx + a\eta - c\epsilon - abx}{b} \\ &\geqq \frac{1}{b}\left(a\lambda - a\left[\frac{b}{|c^*|}\right] - c(|c^*| - 1)\right) \\ &\geqq \frac{1}{b}(a\lambda - M) = -\mu. \end{aligned}$$

We now bound M_0. The case $|c^*| = 1$ yields $a \equiv \pm c \pmod{b}$, which, together with $2a > c > b > a$, shows that a, b, and c form an arithmetic progression. This is in Case I. The case $|c^*| = \frac{1}{2}(c - 2)$ yields $b = c - 1$ and $a \equiv \pm 1 \pmod{b}$. This cannot occur. Hence, we have:

$$F \leqq \frac{ab}{x} + c(x - 1) - 1 \quad \text{with } 2 \leqq x \leqq \tfrac{1}{2}(c - 3).$$

This yields

$$\begin{aligned} F &\leqq \max\left(\tfrac{1}{2}ab + c - 1, \frac{2ab}{c - 3} + \tfrac{1}{2}c(c - 5) - 1\right) \\ &< \tfrac{1}{2}p_e(p_e - 1). \end{aligned}$$

COROLLARY 4.4. *If G is an n-vertex fscdg with $n \geqq 7$ and $p(G) = 1$ and at least three distinct elementary circuit lengths, then*

$$(17) \qquad \gamma(G) \leqq \tfrac{1}{2}n(n + 1).$$

Proof. If the shortest circuit has length at most $\frac{1}{2}n$, the result follows from (11). Let $l > \frac{1}{2}n$ be the length of the shortest circuit. Let d be the length of the shortest path from i to j. If $d \geqq n - l$, then $r_{ij} = d$. If $d < n - l$, we may add an elementary circuit to the path giving $r_{ij} \leqq d + n < 2n - l$. By (9) and (7),

$$\gamma(G) \leqq 2n - l + F(p_1, \ldots, p_e),$$

where p_α $(1 \leqq \alpha \leqq e)$ are the lengths of the elementary circuits of G. In Case I of the proof of the theorem,

$$\gamma(G) < 2n - \tfrac{1}{2}n + \tfrac{1}{2}n(n-2) \leqq \tfrac{1}{2}n(n+1).$$

In Case II of the proof of the theorem, we may take $a = l$ to obtain:

$$\gamma(G) \leqq 2n + \max\left(\frac{ab}{x} + c(x-1) - a - 1\right),$$

where

$$2 \leqq x \leqq \tfrac{1}{2}(c-3), \qquad a < b < c \leqq n, \qquad a + c \neq 2b.$$

This yields (17).

THEOREM 4.5. *Let G be an n-vertex fscdg with exactly two distinct elementary circuit lengths m and s. Assume that $m > s$ and that* $\gcd(m, s) = 1$ *and* $n < m(s-1)$. *Let an elementary m-circuit be*

$$[x_0, x_1, \ldots, x_m = x_0].$$

For some $1 \leqq i \leqq m$, *there is no s-circuit containing* (x_{i-1}, x_i).

Proof. Assume the converse, that for every $1 \leqq i \leqq m$ we have:

$$[x_{i-1}, x_i = y_{1i}, \ldots, y_{si} = x_{i-1}].$$

Not all the y_{ji} $(1 < j \leqq s$ and $1 \leqq i \leqq m)$ are distinct since $n < m(s-1)$. There are two cases both of which lead to contradictions. We begin by establishing:

(**) if $x_u \neq x_v, x_{v-1}$, then there is no circuit of the form $[x_v, \ldots, (?), \ldots, x_u, x_{u+1}, \ldots, (x), \ldots, x_v]$ of length s.

To prove this by contradiction we consider

$$[x_v, \ldots, x_u = y_{1u}, \ldots, y_{su} = x_{u-1} = y_{1,u-1}, \ldots, y_{s,v+1} = x_v],$$

where the first ellipsis corresponds to the first in (**) and the others stand for the obvious y's. Assuming $u < v$, this circuit has length

$$s - (v-u) + (s-1)(m+u-v) = (s-1)m - (v-u-1)s$$

which is impossible since $v > u + 1$ and $\gcd(m, s) = 1$. We now consider the cases mentioned earlier.

https://doi.org/10.4153/CJM-1969-088-3 Published online by Cambridge University Press

Case I: For some i, j, l we have $x_l = y_{ji}$ and $1 < j < s$. Consider the two circuits

$$[x_i = y_{1i}, \ldots, y_{ji} = x_l, \ldots, x_i], \quad [x_l = y_{ji}, \ldots, y_{si} = x_{i-1}, \ldots, x_l].$$

Their lengths add to $m + s$. Hence, one has length s and we may apply (**) to it.

Case II: Case I does not hold.

We have $y_{ji} = y_{kl}$ with $j, k > 1$ and $i \neq l$. By symmetry, $i = l - 1$ may be excluded. Let $y_{ai} = y_{\alpha l}$ be the first of $y_{2i} \ldots, y_{si}$ which equals some y_{kl}, $k > 1$. Let $y_{zi} = y_{\xi l}$ be the last. We have $a \leqq z$. If $\alpha \leqq \xi$, then $\xi - \alpha = z - a$ since no circuits through x_i or x_l can be shorter than s. If $\alpha > \xi$, the circuit

$$[y_{ai}, \ldots, y_{zi} = y_{\xi l}, \ldots, y_{\alpha l} = y_{ai}]$$

has length $(z - a) - (\xi - \alpha)$. In any case, $(z - a) - (\xi - \alpha)$ is a non-negative linear combination of m and s. By (**), the *elementary* circuit

$$[x_i = y_{1i}, \ldots, y_{ai} = y_{\alpha l}, \ldots, y_{sl} = x_{l-1}, \ldots, x_i]$$

has length m. If $l \neq i - 1$, the same reasoning applies to

$$(***) \qquad [x_l = y_{1l}, \ldots, y_{\xi l} = y_{zi}, \ldots, y_{si} = x_{i-1}, \ldots, x_l].$$

Combining we obtain:

$$m + m = (a + s - \alpha) + (\xi + s - z) + m.$$

Thus,

$$(z - a) - (\xi - \alpha) = 2s - m,$$

which is not a non-negative combination of s and m. Hence, $l = i - 1$. But then, replacing (***) by the *elementary* circuit

$$[x_l = y_{1l}, \ldots, y_{\xi l} = y_{zi}, \ldots, y_{si} = x_l]$$

yields

$$m + \begin{cases} m \\ s \end{cases} = (a + (s - \alpha) + 1) + (\xi + (s - z) - 1).$$

Then

$$(z - a) - (\xi - \alpha) = 2s - m - \begin{cases} m \\ s \end{cases} < 0,$$

a contradiction.

We now prove Theorem 4.1. When $n \leqq 8$ we may use (4) and (5). Let G be a graph which gives $x \in \Gamma(n, 1)$ in the statement of the theorem. By (17), G has two distinct elementary circuit lengths, say $m > s$. By (11) we have $2s \geqq n$. Hence, $s + m > n$. Let x_{i-1} and x_i be the vertices mentioned in Theorem 4.5. Then $(x_i; x_{i-1})$ has the upp. By (7) and Theorem 2.2,

$$\gamma(G) \geqq (m - 1) + (ms - m - s) + 1 = (m - 1)s.$$

Let u and v be any vertices. We will show that

$$r_{uv} \leqq n - s - 1 + m.$$

Then by (9) and (7)

$$\begin{aligned} \gamma(G) &\leqq (n - s - 1 + m) + (ms - m - s) + 1 \\ &= (m - 1)s + (m - s) + l, \end{aligned}$$

where $n = m + l$ and $0 \leqq l = n - m < s$; completing the proof. Let d be the distance from u to v. If $d \geqq n - s$, then the corresponding path intersects every circuit and we have

$$r_{uv} = d \leqq n \leqq n - s - 1 + m.$$

If $d < n - s$, we may add an elementary circuit to the path to obtain a path with at least $s \geqq n - s$ distinct vertices. Hence, it intersects every circuit. Thus,

$$r_{uv} \leqq (n - s - 1) + m.$$

References

1. C. Berge, *The theory of graphs and its applications* (Wiley, New York, 1962).
2. A. Brauer and J. E. Schockley, *On a problem of Frobenius*, J. Reine Angew. Math. *211* (1962), 215–220.
3. A. L. Dulmage and N. S. Mendelsohn, *Gaps in the exponent set of primitive matrices*, Illinois J. Math. *8* (1964), 642–656.
4. B. R. Heap and M. S. Lynn, *The structure of powers of non-negative matrices*. I. *The index of convergence* (National Physical Laboratory, Teddington, Middlesex, England, 1964), SIAM J. Appl. Math. *14* (1966), 610–639.
5. R. Z. Norman, private communication.
6. V. Pták and J. Sedláček, *On the index of imprimitivity of non-negative matrices*, Czechoslovak Math. J. *8* (*83*) (1958), 496–501.
7. J. B. Roberts, *Note on linear forms*, Proc. Amer. Math. Soc. *7* (1956), 465–469.
8. T. W. Tucker, *The exponent set of strongly connected graphs*, Senior thesis, Harvard University, 1967.
9. H. Wielandt, *Unzerlegbare, nicht negativen Matrizen*, Math. Z. *52* (1950), 642–648.

Institute for Defense Analyses,
Princeton, New Jersey;
Dartmouth College,
Hanover, New Hampshire