Primitive normal matrices and covering numbers of finite groups

D. Chillag, R. Holzman and I. Yona

Department of Mathematics, Technion, Israel Institute of Technology, Haifa 32000, Israel

Submitted by submitting editor's name

ABSTRACT

A primitive matrix is a square matrix M with nonnegative real entries such that the entries of M^s are all positive for some positive integer s. The smallest such s is called the primitivity index of M. Primitive matrices of normal type (namely: MM^T and M^TM have the same zero entries) occur naturally in studying the so called "conjugacy-class covering number" and "character covering number" of a finite group. We show that if M is a primitive $n \times n$ matrix of normal type with minimal polynomial of degree m, then the primitivity index of M is at most $\left(\left\lceil \frac{n}{2} \right\rceil + 1\right)(m-1)$. This bound is then applied to improve known bounds for the various covering numbers of finite groups.

1. Introduction

A square matrix M over the real number field is called nonnegative (denoted by $M \geq 0$) if all its entries are nonnegative. The matrix is called positive (denoted by $M > 0$) if all its entries are positive. A nonnegative $n \times n$ matrix M is called primitive if $M^s > 0$ for some positive integer s. The smallest such s is called the primitivity index of M and is denoted by $\gamma(M)$. It was shown by Wielandt that $\gamma(M) \leq n^2 - 2n + 2$. This was improved by Shen ([15]) who showed that $\gamma(M) \leq m^2 - 2m + 2$ where m is the degree of the minimal polynomial of M. We say that a matrix M is of symmetric type if M and M^T have exactly the same zero entries. It can be shown ([3], p.47) that if M is a primitive $n \times n$ matrix of symmetric type then $\gamma(M) \leq 2n - 2$. This was improved to $\gamma(M) \leq 2m - 2$ by Hartwig and Neumann ([10]), here again m is the degree of the minimal polynomial of M.

655 Avenue of the Americas, New York, NY 10010 0024-3795/94/$6.00

In this article we discuss another type of matrices with special pattern, namely, matrices of normal type. These are matrices M such that MM^T and M^TM have the same zero entries. We show a bound on $\gamma(M)$ for primitive matrices of normal type which is around half the bound for general primitive matrices.

THEOREM 1.1. *Let M be an $n \times n$ primitive matrix of normal type. Denote by m the degree of the minimal polynomial of M. Then*

$$\gamma(M) \leq \left(\left\lceil \frac{n}{2} \right\rceil + 1 \right) (m-1).$$

Our motivation for studying primitive matrices of normal type, is that they arise naturally in two types of problems in finite group theory.

To explain, we need to set some group theory notation. Let G be a finite group and G' its commutator subgroup. Let A be a subset of G. The subgroup of G generated by A is denoted by $\langle A \rangle$. The product of two subsets A and B of G is defined as $AB = \{ab \mid a \in A, b \in B\}$.

Set $cl(G) = \{C_1 = \{1\}, C_2, C_3, \ldots, C_k\}$ to be the set of all conjugacy classes of G.

Next, let $Irr(G) = \{\chi_1 = 1_G, \chi_2, \ldots, \chi_k\}$ be the set of all ordinary irreducible characters of G. The set of all ordinary characters of G is denoted by $ch(G)$. For $\theta \in ch(G)$, we denote the value of θ on the elements of the conjugacy class C by $\theta(C)$. Set $Z(\theta) = \{g \in G \mid |\theta(g)| = \theta(1)\}$. Furthermore, the set of irreducible constituents of θ is denoted by $Irr(\theta)$.

Let $C \in cl(G)$. The number of distinct numbers in the list (multiset): $\left\{ \frac{\chi(C)}{\chi(1)} \mid \chi \in Irr(G) \right\}$ will be denoted by $m(C)$. The number of distinct values of a character θ will be denoted by $m(\theta)$.

Let $C \in cl(G)$. Then C covers G if $C^s = G$ for some positive integer s, in this case the covering number $cn(C)$ is defined as $cn(C) = \min\{s \mid C^s = G\}$. It can be shown that C covers G if and only if $G = G' = \langle C \rangle$ (See [1], Proposition 3.5).

Let $\theta \in ch(G)$. Then θ covers G if $Irr(\theta^s) = Irr(G)$ for some positive integer s, in this case the character covering number $ccn(\theta)$ is defined as $ccn(\theta) = \min\{s \mid Irr(\theta^s) = Irr(G)\}$. It can be shown that θ covers G if and only if $Z(\theta) = \{1\}$ (See [4], Cor.3.5).

It turns out that the numbers $cn(C)$ and $ccn(\theta)$ are in fact primitivity indices of some primitive matrices that will be defined later. So Theorem 1.1 can be used to bound the covering numbers, as follows.

THEOREM 1.2. *Let G be a finite group with exactly k conjugacy classes. Let C be a conjugacy class of G and θ a character of G. Then:*

1. *If* $G = G' = \langle C \rangle$ *then* $cn(C) \leq \left(\left\lceil \frac{k}{2} \right\rceil + 1\right)(m(C) - 1)$.

2. *If* $Z(\theta) = \{1\}$ *then* $ccn(\theta) \leq \left(\left\lceil \frac{k}{2} \right\rceil + 1\right)(m(\theta) - 1)$.

Using group theoretic considerations it was shown that if G is a finite nonabelian simple group then (see [1]) $cn(C) \leq \frac{4}{9}k^2$ for every $C \in cl(G) - \{\{1\}\}$, and (see [2]) $ccn(\theta) \leq \frac{1}{2}k^2$ for every $\theta \in Irr(G) - \{1_G\}$; here k is the number of conjugacy classes of G. In general $m(C)$ and $m(\theta)$ are no bigger than k, and in many cases they are much smaller than k. So the bounds in Theorem 1.2 are better than the known ones for many cases. The main point, however, is that the bounds in Theorem 1.2 are achieved with no group theory consideration at all. They are consequences of Theorem 1.1. In fact the two bounds will be deduced from a bound on a covering number of elements of so called "algebras with positive bases", of which classes and characters are special cases. These algebras were introduced in [5] where primitive matrices were used to conclude that $cn(C) \leq m(C)^2 - 2m(C) + 2$ and $ccn(\theta) \leq m(\theta)^2 - 2m(\theta) + 2$.

The structure of the paper is as follows. Theorem 1.1 will be proved in section 2. In section 3 we collect the relevant facts on algebras with positive bases and apply Theorem 1.1 to bound covering numbers in the algebra. Theorem 1.2 will be deduced from the bound of section 3 in section 4. In the last section we will use primitive matrices to bound covering numbers for special conjugacy classes (classes of commutators) and special characters (characters that have a common constituent with the conjugacy character), and discuss their significance and resemblance.

2. Primitive matrices of normal type

Let M be a nonnegative matrix. The Perron-Frobenius theorem (see [3], chapter 2) states that the spectral radius $\rho(M)$ of M is an eigenvalue of M. The matrix M is called irreducible if for every pair of indices i, j there exists a positive integer $s(i, j)$ such that the i, j - th entry of $M^{s(i,j)}$ is positive (see [3], Chapter 2, (1.2) and (2.1)). Clearly, every primitive matrix is irreducible. The number of eigenvalues of an irreducible matrix M whose absolute value is equal to $\rho(M)$ is called the imprimitivity index (or the cyclicity index) of M.

The i, j - th entry of a matrix A will be denoted by $(A)_{ij}$.

The directed graph $G(M)$ of the nonnegative $n \times n$ matrix M is defined to have the numbers $1, 2, 3, \ldots, n$ as vertices, and an edge (i, j) exists if and only if $a_{ij} \neq 0$. The set of edges of $G(M)$ will be denoted by $E(M)$. A nonnegative matrix M is irreducible if and only if $G(M)$ is strongly connected, i.e., for any pair of vertices i, j, there is a path in $G(M)$ connecting i to j (see [3], p. 30).

The index of primitivity $\gamma(M)$ of a primitive $n \times n$ matrix $M = (m_{ij})$ is closely related to the lengths of the cycles of $G(M)$.

PROPOSITION 2.1. *Let M be a nonnegative square matrix.*

1. *If M is primitive then the g.c.d of all the lengths of cycles in $G(M)$ is equal to* 1.
2. *Suppose that M is of normal type. Then for any two given vertices u and v, there exists a vertex x such that $\{(x, u), (x, v)\} \subset E(M)$ if and only if there exists a vertex y such that $\{(u, y), (v, y)\} \subset E(M)$.*

Proof. 1. This is well known and follows from the following facts. Since M is primitive, its imprimitivity index is equal to 1 (see [12], chapter III, definition 1.1 and Theorem 2.1). As M is irreducible, $G(M)$ is strongly connected and by 3.4 and 3.5 of chapter 4 of [12], the *g.c.d* of all lengths of circuits of $G(M)$ is equal to the imprimitivity index (which is equal to 1) of M.

2. Let n be the order of M and set $M = (m_{ij})$. Let u and v be two vertices for which there is a vertex y such that $\{(u, y), (v, y)\} \subset E(M)$. This means that $m_{uy} > 0$ and that $m_{vy} > 0$. It follows that

$$\left(MM^T\right)_{uv} = \sum_{k=1}^{n} (M)_{uk}(M^T)_{kv} = \sum_{k=1}^{n} m_{uk}m_{vk} > 0.$$

Since M is of normal type $\left(M^T M\right)_{uv} > 0$. Therefore:

$$\left(M^T M\right)_{uv} = \sum_{k=1}^{n} (M^T)_{uk}(M)_{kv} = \sum_{k=1}^{n} m_{ku}m_{kv} > 0.$$

Hence, there exists an index x such that $m_{xu} > 0$ and $m_{xv} > 0$, implying that $\{(x, u), (x, v)\} \subset E(M)$. The other direction is proved similarly.

Hartwig and Neumann proved:

THEOREM 2.1. *([10]) Let M be a primitive matrix, m the degree of its minimal polynomial and g the length of the shortest cycle of the graph $G(M)$. Then $\gamma(M) \leq (m-1)(g+1)$.*

Now Theorem 1.1 is a direct consequence of Proposition 2.1, Theorem 2.1 and the following theorem. (Note that assumptions 1 and 2 in this theorem are weaker versions of the corresponding conclusions in Proposition 2.1.)

THEOREM 2.2. *Let G be a directed graph with n vertices. Let E be the set of edges of G. Assume that:*

1. *G has at least two cycles of distinct lengths.*
2. *Whenever for two vertices u and v, there exists a vertex x such that $\{(x,u),(x,v)\} \subset E$, then there exists a vertex y such that $\{(u,y),\ (v,y)\} \subset E$.*

Then G has a cycle of length at most $\lceil \frac{n}{2} \rceil$.

Proof. Recall that a walk in a directed graph is a finite sequence of vertices $u_0 \to u_1 \to \cdots \to u_k$ where the arrows indicate the existence of an edge from u_{i-1} to u_i, $i = 1, \ldots, k$. There is no restriction on multiple appearances of vertices and edges along the walk. The vertices u_0 and u_k are called the origin and the terminus of the walk, respectively, and k is the length of the walk.

A pair of walks P and Q that have the same origin and the same terminus will be called a bi-walk. We will refer to it as a k,l-bi-walk where k is the length of P and l is the length of Q. Thus, in a k,l-bi-walk we have a common origin w and a common terminus z, and the two walks are of the form

$$\begin{aligned} P &: \quad w = u_0 \to u_1 \to \cdots \to u_{k-1} \to u_k = z \\ Q &: \quad w = v_0 \to v_1 \to \cdots \to v_{l-1} \to v_l = z \end{aligned}$$

We will be interested in k,l-bi-walks with $1 \leq l - k \leq \lceil \frac{n-3}{2} \rceil$. Such bi-walks will be called admissible.

Suppose that the directed graph G satisfies the assumptions of the theorem, but has no cycle of length at most $\lceil \frac{n}{2} \rceil$. We proceed in several steps.

Step 1. We show that there exists at least one admissible bi-walk.

By assumption, G has two cycles whose lengths k and l satisfy $\lceil \frac{n}{2} \rceil < k < l \leq n$. Since $k + l > n$, the two cycles must have at least one vertex

in common. For such a vertex t, consider the walk P that goes from t to t along the shorter of the two cycles, and the walk Q that goes from t to t along the longer cycle. The two walks form a k,l-bi-walk. It is admissible because $1 \leq l-k \leq n - \left\lceil \frac{n}{2} \right\rceil - 1 = \left\lceil \frac{n-3}{2} \right\rceil$.

Now, we select among the admissible bi-walks in G one

$$\begin{aligned} P &: \quad w = u_0 \to u_1 \to \cdots \to u_{k-1} \to u_k = z \\ Q &: \quad w = v_0 \to v_1 \to \cdots \to v_{l-1} \to v_l = z \end{aligned}$$

that is minimal, in the sense that it has the smallest possible k. If $k = 0$ then $w = z$ and Q is a closed walk of length $l \leq \left\lceil \frac{n-3}{2} \right\rceil$, which contradicts the absence of cycles of length at most $\left\lceil \frac{n}{2} \right\rceil$. Thus, $k \geq 1$.

Step 2. Given a minimal admissible k,l-bi-walk P,Q as above, we present a construction that produces another minimal admissible k,l-bi-walk P',Q'.

Consider P and Q as above. By assumption, since $\{(w,u_1),(w,v_1)\} \subset E$, there exists a vertex, say y_1, such that $\{(u_1,y_1),(v_1,y_1)\} \subset E$.

Assuming $k \geq 2$, we repeat the argument with $\{(u_1,u_2),(u_1,y_1)\} \subset E$ and deduce that there exists a vertex y_2 such that $\{(u_2,y_2),(y_1,y_2)\} \subset E$. In general, we iterate that argument k times and find vertices $y_1, y_2, \ldots, y_k$ such that

$$\{(u_i,y_i) \,|\, i = 1,\ldots,k\} \subset E \text{ and } \{(v_1,y_1)\} \cup \{(y_{i-1},y_i) \,|\, i = 2,\ldots,k\} \subset E.$$

Now the two walks

$$\begin{aligned} P' &: \quad v_1 \to y_1 \to \cdots \to y_{k-1} \to y_k \\ Q' &: \quad v_1 \to v_2 \to \cdots \to v_l = u_k \to y_k \end{aligned}$$

form another k,l-bi-walk, as promised.

We note that if $k \geq 2$ then y_{k-1} must be distinct from u_k, since otherwise we could truncate the two walks P',Q' to obtain a $k-1,l-1$-bi-walk, contradicting the minimality of k.

Clearly we may iterate the above construction to obtain from P',Q' another minimal admissible k,l-bi-walk P'',Q'' and so on. In general, starting from $(P_0,Q_0) = (P,Q)$ we get an infinite sequence of minimal admissible bi-walks P_i,Q_i, $i = 0,1,2,\ldots$.

Let us denote by t_i and z_i the next-to-last and the last vertex, respectively, in the walk P_i. In terms of our previous notation, we have:

$t_0 = u_{k-1}$

$z_0 = u_k$

$t_1 = \begin{cases} y_{k-1} & \text{if } k \geq 2 \\ v_1 & \text{if } k = 1 \end{cases}$

$z_1 = y_k$.

It follows from the construction that all the edges indicated by arrows in the following diagram do exist in G:

$$\begin{array}{ccc} t_0 & \longrightarrow & z_0 \\ \downarrow & & \downarrow \\ t_1 & \longrightarrow & z_1 \\ \downarrow & & \downarrow \\ t_2 & \longrightarrow & z_2 \\ & \vdots & \end{array}$$

.

Step 3. We show that unless $k = 1$, the first $\left\lceil \frac{n+1}{2} \right\rceil$ rows in the above diagram contain a cycle of length at most $\left\lceil \frac{n}{2} \right\rceil$.

Indeed, by the pigeonhole principle some vertex must appear twice in the first $\left\lceil \frac{n+1}{2} \right\rceil$ rows of the diagram. If such a double appearance occurs in the same column, it yields a cycle of length at most $\left\lceil \frac{n-1}{2} \right\rceil$.

Next, suppose that there is a double appearance of the form $t_i = z_j$ with $i \leq j$. This yields a cycle of length $j - i + 1 \leq \left\lceil \frac{n+1}{2} \right\rceil$, and so we are done unless n is even, $i = 0$ and $j = \frac{n}{2}$. However, when n is even $2\left\lceil \frac{n+1}{2} \right\rceil = n+2$ and hence this cannot be the only double appearance. It remains to deal with the case of a double appearance of the form $t_i = z_j$ with $i > j$. We claim that in this case $k = 1$. Indeed, we have the $1, (i-j)$-bi-walk

$$\begin{aligned} P^* &: \quad t_i \to z_i \\ Q^* &: \quad z_j \to z_{j+1} \to \cdots \to z_{i-1} \to z_i. \end{aligned}$$

As noted at the end of step 2, if $k \geq 2$ we have $t_{j+1} \neq z_j$, which implies that $i - j \geq 2$. On the other hand, we have $i - j \leq \left\lceil \frac{n-1}{2} \right\rceil$. It follows that if $k \geq 2$ then $1 \leq (i-j) - 1 \leq \left\lceil \frac{n-3}{2} \right\rceil$, and therefore P^*, Q^* is an admissible bi-walk, which contradicts the minimality of k. Hence $k = 1$.

Step 4. We show that if $k = 1$ then $t_{i+l} = z_i$ for $i = 0, 1, 2, \ldots$.

Recalling our earlier notation for the bi-walks P, Q and P', Q' in step 2, when $k = 1$ we have $t_1 = v_1$, i.e., it is the second vertex on Q. Similarly, t_2 is the second vertex on Q', which is v_2, the third vertex on Q. Continuing like this, we get that t_l is the $(l+1)$-th vertex on Q, which is v_l which in turn is z_0. Thus $t_l = z_0$, and similarly $t_{l+1} = z_1$, and so on.

Step 5. We show that if $k = 1$ then the first $n + 1$ rows in the above diagram contain a cycle of length at most $\left\lceil \frac{n}{2} \right\rceil$.

By the pigeonhole principle, some vertex must appear twice in the left column within the first $n+1$ rows. Say $t_{h+d} = t_h$ for some $1 \leq d \leq n$. The existence of an edge from t_i to z_i means, by step 4, that there is an edge from t_i to t_{i+l} for every i. Hence we have a closed walk of the form

$$t_h \to t_{h+l} \to \cdots \to t_{h+\left\lfloor \frac{d}{l} \right\rfloor l} \to t_{h+\left\lfloor \frac{d}{l} \right\rfloor l+1} \to \cdots \to t_{h+d} \ .$$

We will show that the length of this closed walk is no more than $\lceil \frac{n}{2} \rceil$. Thinking of n and l as fixed and d as a variable, the above closed walk is longest when d is of the form $d = sl - 1$, where s is the largest integer such that $sl - 1 \leq n$. Thus it suffices to show that $s + l - 2 \leq \lceil \frac{n}{2} \rceil$ subject to the conditions $sl - 1 \leq n$ and $2 \leq l \leq \lceil \frac{n-1}{2} \rceil$. It is easy to see that only the extreme values of l need to be considered.

For $l = 2$ we have $2s - 1 \leq n$, and therefore $s + l - 2 = s \leq \lceil \frac{n}{2} \rceil$. Next suppose that $l = \lceil \frac{n-1}{2} \rceil$. Then $s + l - 2 \leq \lceil \frac{n}{2} \rceil$ if $s \leq 2$ or $s = 3$ and n is odd. These conditions must hold true given that $s \lceil \frac{n-1}{2} \rceil - 1 \leq n$, as long as $n \geq 4$. In the remaining cases, when $n \leq 3$, our theorem is trivially true.

This completes the proof of Theorem 2.2.

We remark that the bound given in the above theorem is the best possible. Indeed, consider the directed graph G with vertices $0, 1, \ldots, n-1$ and edges $(i, i+1)$, $(i, i+2)$, $i = 0, 1, \ldots, n-1$ (where addition is modulo n). This graph satisfies the conditions of the theorem (in fact, even in their stronger versions as they appear in Proposition 2.1), and its shortest cycle has length $\lceil \frac{n}{2} \rceil$. However, we do not know if the bound on the primitivity index for normal type matrices given in Theorem 1.1 is optimal (or even close to being optimal). The matrix that corresponds to the above example G has primitivity index $n - 1$, whereas the upper bound is quadratic in n.

3. Covering numbers in algebras with positive bases

In this section we summarize the facts on algebras with positive bases that are needed.

Let $\mathbb{F}$ be any subfield of the real number field $\mathbb{R}$ and let $\mathbf{A}$ be a semisimple, finite-dimensional commutative $\mathbb{F}$-algebra. The identity element of $\mathbf{A}$ (which is known to exist) will be denoted by $1_{\mathbf{A}}$. Let $\mathfrak{B} = \{b_1 = 1_{\mathbf{A}}, b_2, ..., b_n\}$ be a basis of $\mathbf{A}$. The structure constants of $\mathfrak{B}$ are the numbers α_{ijk} defined by the equations: $b_i b_j = \sum_{k=1}^{n} \alpha_{ijk} b_k$. If all the structure constants of $\mathfrak{B}$ are nonnegative real numbers we say that $\mathfrak{B}$ is a nonnegative basis of $\mathbf{A}$.

A nonzero element $a = \sum_{i=1}^{n} \alpha_i b_i$ of $\mathbf{A}$ is called a nonnegative element, if each α_i is a nonnegative real number.

For every $a \in \mathbf{A}$, let $M(a, \mathfrak{B}) = (m_{ij}(a, \mathfrak{B}))$ be the $n \times n$ matrix whose entries $m_{ij}(a, \mathfrak{B})$ are given by the equations: $ab_i = \sum_{j=1}^{n} m_{ij}(a, \mathfrak{B}) b_j$.

So, $\mathfrak{B}$ is a nonnegative basis, if and only if all entries of all the matrices $M(b_i, \mathfrak{B})$ are nonnegative. Also, if $\mathfrak{B}$ is a nonnegative basis and $a \in \mathbf{A}$ is a nonnegative element, then the matrix $M(a, \mathfrak{B})$ is nonnegative. By ([3] (1.1) chapter 2), both matrices $M(a, \mathfrak{B})$ and $(M(a, \mathfrak{B}))^T$ have nonnegative eigenvectors corresponding to $\rho(a) \stackrel{\circ}{=} \rho(M(a, \mathfrak{B})) = \rho(M(a, \mathfrak{B}))^T$.

DEFINITION 3.1. A pair ($\mathbf{A}$,$\mathfrak{B}$) is called an algebra with a positive basis if $\mathfrak{B}$ is a basis of the semi-simple, finite-dimensional commutative $\mathbb{F}$-algebra $\mathbf{A}$ (where $\mathbb{F}$ is a subfield of the real number field), and the following two conditions are satisfied:

1. The structure constants of $\mathfrak{B}$ are nonnegative.
2. For every nonnegative element $a \in \mathbf{A}$, each of the matrices $M(a, \mathfrak{B})$ and $(M(a, \mathfrak{B}))^T$ has a **positive** eigenvector corresponding to $\rho(a)$.

Let ($\mathbf{A}$,$\mathfrak{B}$) be an algebra with a positive basis $\mathfrak{B} = \{b_1 = 1_{\mathbf{A}}, b_2, ..., b_n\}$. Then $M(c, \mathfrak{B})M(d, \mathfrak{B}) = M(cd, \mathfrak{B}) = M(d, \mathfrak{B})M(c, \mathfrak{B})$ and $M(a, \mathfrak{B})$ is diagonalizable for all $a, c, d \in \mathbf{A}$ (see [6], lemma 2.1).

Let $a \in \mathbf{A}$. Then the support of a is denoted by $Irr(a)$. Namely, if we write $a = \sum_{i=1}^{n} \alpha_i b_i$, then $Irr(a) = \{b_i \mid \alpha_i \neq 0\}$.

Suppose that $a \in \mathbf{A}$ is nonnegative. Denote by $z(a)$ the number of eigenvalues of $M(a, \mathfrak{B})$ whose absolute value is equal to $\rho(a)$.

The covering number $cn(a)$ of a nonnegative $a \in \mathbf{A}$ is defined as follows:

$$cn(a) = \min \{s \mid Irr(a^s) = \mathfrak{B}\}.$$

Of course, $cn(a)$ may not exist.

A connection between covering numbers and primitive matrices was given in [5].

THEOREM 3.1. *([5], Theorem 4.2d) Let* ($\mathbf{A}$,$\mathfrak{B}$) *be an algebra with a positive basis, and let* $a \in \mathbf{A}$ *be nonnegative. Then*

1. $cn(a)$ *exists if and only if* $z(a) = 1$.
2. $cn(a)$ *exists if and only if the matrix* $M(a, \mathfrak{B})$ *is primitive, and* $cn(a)$ *is equal to the primitivity index of* $M(a, \mathfrak{B})$.

From Theorem 3.1 and our main Theorem (1.1) we conclude:

COROLLARY 3.1. *Let* $(\mathbf{A},\mathfrak{B})$ *be an* n*-dimensional algebra with a positive basis, and let* $a \in \mathbf{A}$ *be nonnegative with* $z(a) = 1$*. Assume that* $M(a,\mathfrak{B})$ *is of normal type, and let* m *be the number of distinct eigenvalues of* $M(a, \mathfrak{B})$*. Then* $cn(a) \leq (m-1)(\lceil \frac{n}{2} \rceil + 1)$*.*

Proof. The matrix $M(a, \mathfrak{B})$ is diagonalizable. Thus, the number of distinct eigenvalues of $M(a, \mathfrak{B})$ is equal to the degree of its minimal polynomial. By the assumption and Theorem 3.1, $M(a, \mathfrak{B})$ is primitive of normal type, with primitivity index equal to $cn(a)$. Now Theorem 1.1 implies that $cn(a) \leq (m-1)(\lceil \frac{n}{2} \rceil + 1)$.

4. Covering numbers in finite groups

Theorem 1.2 is proved by applying Theorem 1.1 to two specific algebras with positive bases arising in finite group theory. In the following G is a finite group, keeping the notation of the introduction. We first collect the facts on these algebras that will be used. They are taken from examples 1.6, 1.7, 5.1 and 5.2 of [5] and Proposition 3.3 of [7].

We denote by $\mathbb{Q}Irr(G)$ the algebra generated by $Irr(G)$ over the field of rational numbers $\mathbb{Q}$. Then $Irr(G)$ is a positive basis for the algebra with positive basis $(\mathbb{Q}Irr(G), Irr(G))$. Let θ be an ordinary character of G. Then θ is a nonnegative element of $\mathbb{Q}Irr(G)$. Moreover, $M(\theta) \triangleq M(\theta, Irr(G)) = ([\theta\chi_i, \chi_j])$ (here $[\cdot,\cdot]$ is the inner product of the characters) and the eigenvalues of $M(\theta)$ are $\rho(M(\theta)) = \theta(1), \theta(C_2), \ldots, \theta(C_k)$. Furthermore, $z(\theta) = 1$ if and only if $Z(\theta) = \{1\}$, and $(M(\theta))^T = M(\overline{\theta})$ where $\overline{\theta}$ is the complex conjugate of θ.

For every $C \in cl(G)$ let $\overline{C} = \sum_{x \in C} x$ be the class sum of C in the group algebra $\mathbb{Q}G$. The set $cls(G) = \left\{\overline{C} \mid C \in cl(G)\right\}$ is a basis of the center $Z(\mathbb{Q}G)$ of $\mathbb{Q}G$. In fact $cls(G)$ is a positive basis of the algebra with positive basis $(Z(\mathbb{Q}G), cls(G))$. For $C \in cl(G)$ let $M(C) \triangleq M(\overline{C}, cls(G)) = (m_{ij}(C))$. It is well known that $m_{ij}(C)$ is the number of ways a given element of C_j can be expressed as a product ab where $a \in C$ and $b \in C_i$ (see [11] proof of 2.4). The eigenvalues of $M(C)$ are the numbers $\rho(M(C)) =$

$|C| = \frac{|C|\chi_1(C)}{\chi_1(1)}, \frac{|C|\chi_2(C)}{\chi_2(1)}, \ldots, \frac{|C|\chi_k(C)}{\chi_k(1)}$. Furthermore $z(\overline{C}) = 1$ is equivalent to $G = G' = \langle C \rangle$ and $(M(C))^T = \left(m_{ij}(C^{-1})\frac{|C_j|}{|Ci|}\right)$ where C^{-1} is the conjugacy class consisting of the inverses of the elements of C.

PROPOSITION 4.1. *Let G be a finite group, C a conjugacy class of G and θ a character of G. Then the matrices $M(C)$ and $M(\theta)$ are of normal type.*

Proof. Let k be the number of conjugacy classes of G.

Since $M(\theta)$ commutes with $M(\overline{\theta}) = (M(\theta))^T$ we get that $M(\theta)$ is in fact a normal matrix.

Since

$$t_{ij} \stackrel{\circ}{=} \left(M(C)\left(M(C)^T\right)\right)_{ij} = \sum_{r=1}^{k} m_{ir}(C)m_{rj}(C^{-1})\frac{|C_j|}{|C_r|}$$

we get that $t_{ij} \neq 0$ if and only if $m_{ir}(C)m_{rj}(C^{-1})\frac{|C_j|}{|C_r|} \neq 0$ for some r, which is equivalent to $m_{ir}(C)m_{rj}(C^{-1}) \neq 0$, since $\frac{|C_j|}{|C_r|} \neq 0$. Thus $t_{ij} \neq 0$ is equivalent to $\left(M(C)M(C^{-1})\right)_{ij} \neq 0$. Since $M(C)$ and $M(C^{-1})$ commute, $t_{ij} \neq 0$ is equivalent to $\left(M(C^{-1})M(C)\right)_{ij} \neq 0$ which in turn is equivalent to $m_{is}(C^{-1})m_{sj}(C) \neq 0$ for some s. Since $\frac{|C_s|}{|Ci|} \neq 0$, this is equivalent to $m_{is}(C^{-1})\frac{|C_s|}{|Ci|} \cdot m_{sj}(C) \neq 0$ which is the same as $\left(\left(M(C)^T\right)M(C)\right)_{ij} \neq 0$.

Next we prove Thereom 1.2.

Proof. 1. Recall that $\overline{C}$ is a nonnegative element of the algebra with positive basis $(Z(\mathbb{Q}G), cls(G))$. By assumption $G = G' = \langle C \rangle$ which implies that $z(\overline{C}) = 1$. By Theorem 3.1, $cn(\overline{C})$ exists and it is equal to the primitivity index of the primitive matrix $M(C)$. The number of distinct eigenvalues of $M(C)$ is $m(C)$. The previous proposition implies that $M(C)$ is of normal type so by Corollary 3.1 we get that $cn(\overline{C}) \leq (m(C)-1)(\lceil \frac{k}{2} \rceil + 1)$.

It is well known that the following two statements for a natural number s are equivalent: i. $\left(\overline{C}\right)^s = \sum_{D \in cl(G)} \alpha_D \overline{D}$ with all $\alpha_D > 0$, and ii. $C^s = G$. To see this, set $D = \left\{g_1^D, g_2^D, \ldots, g_{l(D)}^D\right\}$ for each $D \in cl(G)$. Rewrite i. as:

$$\left(g_1^C + g_2^C + \ldots + g_{l(C)}^C\right)^s = \sum_{D \in cl(G)} \alpha_D \left(g_1^D + g_2^D + \ldots + g_{l(D)}^D\right).$$

So $\alpha_D > 0$ if and only if an element $d \in D$ can be written as a product of exactly s elements of C, which is the same as $d \in C^s$. So i. is equivalent

to ii., which implies that $cn(\overline{C})$ is the same as $cn(C)$ as defined in the introduction.

2. Recall that θ is a nonnegative element of the algebra with positive basis $(\mathbb{Q}Irr(G), Irr(G))$. By assumption $Z(\theta) = \{1\}$ which implies that $z(\theta) = 1$. By Theorem 3.1 $cn(\theta)$ exists and it is equal to the primitivity index of the primitive matrix $M(\theta)$. The number of distinct eigenvalues of $M(\theta)$ is $m(\theta)$. The previous proposition implies that $M(\theta)$ is of normal type so by Corollary 3.1 we get that $cn(\theta) \leq (m(\theta) - 1)(\lceil \frac{k}{2} \rceil + 1)$. Note that $cn(\theta)$ is the same as $ccn(\theta)$ as defined in the introduction.

5. Commutators and the conjugacy character

Suppose that M is a primitive $n \times n$ matrix with a nonzero trace. Then $G(M)$ has a loop (circuit of length 1) and Hartwig and Neumann's Theorem (2.1), implies that the primitivity index of M is no bigger than $2(m-1) \leq 2(n-1)$, where m is the degree of the minimal polynomial of M. In this section we comment on covering numbers for conjugacy classes C and characters θ for which the traces of $M(C)$ and $M(\theta)$ are nonzero and explain the significance of such classes and characters.

We recall that a commutator in the group G is an element of the form $x^{-1}y^{-1}xy$ and the conjugacy character is the function $\tau_G : g \mapsto |C_G(g)|$ for all $g \in G$. Here $C_G(g)$ is the centralizer in G of g. The second orthogonality relation on characters states: $\tau_G = \sum_{\chi \in Irr(G)} \chi\overline{\chi}$, where $\overline{\chi}$ is the complex conjugate of χ.

The first observation is:

PROPOSITION 5.1. *Let G be a finite group, C a conjugacy class of G and θ a character of G. Then*

1. *$tr(M(C)) \neq 0$ if and only if C consists of commutators.*
2. *$tr(M(\theta)) \neq 0$ if and only if θ has a common constituent with the conjugacy character, i.e., $Irr(\theta) \cap Irr(\tau_G)$ is not empty.*

Proof. As usual we set $cl(G) = \{C_1 = \{1\}, C_2, \ldots, C_k\}$, and $Irr(G) = \{\chi_1 = 1_G, \chi_2, \ldots, \chi_k\}$.

1. $tr(M(C)) \neq 0$ implies that $m_{ii}(C) > 0$ for some i which is the same as $C_i \subset C_iC$. Let $g \in C_i$, then $g = g_1h$ for some $g_1 \in C_i$ and $h \in C$. As g_1

is conjugate to g we can write $g_1 = x^{-1}gx$ for some $x \in G$. So $g = x^{-1}gxh$ and so $h = x^{-1}g^{-1}xg$ is a commutator. As all elements of C are conjugate, and conjugates of commutators are commutators we get that C consists of commutators.

Conversely, suppose that C consists of commutators. Let $y \in C$, then $y = a^{-1}b^{-1}ab$ for some $a, b \in G$ which is the same as $ay = b^{-1}ab$. Let C_j be the conjugacy class of a, then element $b^{-1}ab$ of C_j is contained in C_jC. So all conjugates of $b^{-1}ab$ are in C_jC implying $C_j \subset C_jC$. Therefore $m_{jj}(C) > 0$.

2. $tr(M(\theta)) \neq 0$ means that $m_{ii}(\theta) > 0$ for some i which is the same as $\chi_i \in Irr(\theta\chi_i)$. This is equivalent to $[\theta\chi_i, \chi_i] = [\theta, \chi_i\overline{\chi_i}] \neq 0$ which is equivalent to $Irr(\theta) \cap Irr(\tau_G)$ being nonempty.

From Proposition 5.1 we see that for a class C of commutators and for a constituent θ of the conjugacy character the covering number (when it exists) is no bigger than $2m-2 \leq 2k-2$ (where $m = m(C)$ or $m(\theta)$ respectively). The bound $2k-2$ can be lowered if C is a class of commutators (respectively θ is a constituent of the conjugacy character) in more than one way.

An element g of the group G is a commutator if and only $g \in C^{-1}C$ for some conjugacy C of G. The number of such C 's influences the covering number of the conjugacy class of g.

Similarly, for a character θ, having a common constituent with the conjugacy character, means that θ has a common constituent with $\chi\overline{\chi}$ for some $\chi \in Irr(G)$. The number of such χ's influences $ccn(\theta)$.

PROPOSITION 5.2. *Let G be a finite group with exactly k conjugacy classes.*

1. *Let D be a conjugacy class such that $\langle D\rangle = G' = G$. Assume that there are $d \geq 1$ conjugacy classes C such that $D \subset C^{-1}C$. Then $cn(D) \leq 2k-1-d$.*

2. *Let θ be an ordinary character such that $Z(\theta) = \{1\}$. Assume that there are $d \geq 1$ irreducible characters χ such that $[\theta, \chi\overline{\chi}] \neq 0$. Then $ccn(\theta) \leq 2k-1-d$.*

Proof. Let the C_i's and χ_j's be as in the proof of Propostion 5.1.

1. Suppose that $D \subset C_i^{-1}C_i$. Let $d \in D$, then $d = c^{-1}x^{-1}cx$ for some $c \in C_i$ and $x \in G$. Thus $x^{-1}cx = cd \in C_iD$ and since C_iD is a normal subset we get that $C_i \subset C_iD$. Therefore $m_{ii}(D) > 0$. By assumption there are at least d positive diagonal entries in $M(D)$. Now the result follows from Corollary 4.8, p. 47 of [3].

2. Suppose that $[\theta, \chi_i\overline{\chi}_i] \neq 0$. Then $[\theta\chi_i, \chi_i] \neq 0$ so that $\chi_i \in Irr(\theta\chi_i)$ which implies that $m_{ii}(\theta) > 0$. By assumption there are at least d positive diagonal entries in $M(\theta)$. Now the result follows from Corollary 4.8, p. 47 of [3].

The significance of better bounds for commutators lies in Ore's conjecture stating that in a nonabelian finite simple group every element is a commutator. This conjecture was proved for almost all finite nonabelian simple groups. Ore proved it for the alternating groups ([14]), Neubuser, Pahlings and Cleuvers ([13]) for the sporadic groups and Ellers and Gordeev ([8]) proved it for groups of Lie type over fields with more than 8 elements. In fact Ellers and Gordeev dealt with many cases where the field has 8 elements or less (actually, a stronger conjecture (Thompson's) was verified in [13] and [8]). Furthermore, the conjecture was verified for some groups of Lie type over all finite fields (see the introduction of [8] for a list). From this we get:

THEOREM 5.1. *Let G be a finite nonabelian simple group with exactly k conjugacy classes. Let C be any nonidentity conjugacy class of G. Then either G is a group of Lie type over a field with less than nine elements or $cn(C) \leq 2m(C) - 2 \leq 2k - 2$.*

As mentioned above, the bound is known to be true for many cases of Lie groups over fields with less than nine elements as well.

For constituents of the conjugacy character, it is not true that every irreducible character of a finite nonabelian simple group is a constituent of the conjugacy character; the character of degree 6 of $PSU(3,3)$ is an example (given by Frame).

QUESTION. In which finite nonabelian simple groups is every irreducible character a constituent of the conjugacy character?

The alternating groups are such groups, as shown by A.Mann (unpublished).

REFERENCES

1 Z. Arad, M. Herzog and J. Stavi, Powers and products of conjugacy classes in groups. Lecture Notes in Math., vol 1112, Springer 1985.

2 Z. Arad and H. Lipman-Gutweter, On products of characters in finite groups. Houston J. Math. 15 (1989), no. 3, 305–326.

3 A. Berman and R. J. Plemmons, Nonnegative Matrices in the Mathematical Sciences, Academic Press, New York, 1979.

4 D. Chillag, Characters, nonnegative matrices, and generalized circulants, Proc. of Symposia in Pure Math., AMS, 47 (1987), 33-40.

5 D. Chillag, Semisimple commutative algebras with positive bases. J. Algebra 210 (1998), no. 1, 242–270.

6 D. Chillag, Regular representations of semisimple algebras, separable field extensions, group characters, generalized circulants, and generalized cyclic codes, Linear Algebra and its Applications 218 (1995), 147-183.

7 D. Chillag, Nonnegative matrices, Brauer characters, normal subsets, and powers of representation modules, Linear Algebra and its Applications 157 (1991), 69-99.

8 E. W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore, Trans. Amer. Math. Soc. 350 (9) (1998), 3657–3671.

9 E. W. Ellers, N. L. Gordeev and M. Herzog, Covering numbers for Chevalley groups, Israel J. Math. 111 (1999), 339–372.

10 R. E. Hartwig and M. Neumann, Bounds on the exponent of primitivity which depend on the spectrum and the minimal polynomial. Linear Algebra and its Appl. 184 (1993), 103-122.

11 I. M. Isaacs, Character Theory of Finite Groups, Academic Press, 1976.

12 H. Minc, Nonnegative Matrices, John Wiley and Sons, New York, 1988.

13 J. Neubuser, H. Pahlings and E. Cleuvers, Each sporadic finasig G has a class C such that $CC = G$, Abstracts AMS 5 (1984), 395.

14 O. Ore, Some remarks on commutators, Proc. Amer. Math. Soc. 272 (1951), 307–314.

15 J. Shen, Proof of a conjecture about the exponent of primitive matrices, Linear Algebra and its Appl. 216 (1995), 185-203.