The commuting graphs of finite rings

By DAVID DOLŽAN (Ljubljana)

Abstract. In this paper, we investigate connectivity and diameters of commuting graphs of finite rings. In case of a directly decomposable ring, we calculate the diameter depending on the diameters of commuting graphs of direct summands. If the ring is indecomposable, we examine the connectedness of the commuting graph according to the number of isomorphic minimal idempotents.

1. Introduction

Commutativity is a well-studied and important concept in the theory of groups and rings. One approach to studying this property is to associate certain graphs to these algebraic structures. This approach can be traced back at least as far as Brauer and Fowler [4], in their attempt towards the classification of simple finite groups. More precisely, given an algebraic structure $A$, one lets $\Gamma = \Gamma(A)$ be a simple (that is, has no loops or multiple edges) undirected graph, with its vertex set equal to all the noncentral elements from $A$, and where two distinct vertices form an edge if the corresponding elements commute in $A$. We remark that for abelian algebras, the corresponding commuting graph is empty (has no vertices).

The commutativity relation sometimes suffices to determine the given algebraic structure up to an isomorphism. If one knows the isomorphism type of the commuting graph of an algebra, then one can often deduce certain properties of that algebra. For example, Solomon and Woldar [9] showed that if the

---

Mathematics Subject Classification: 16P10, 16N20, 05C12.

Key words and phrases: commuting graph, finite ring, connected graph, diameter.

The author acknowledges the financial support from the Slovenian Research Agency (research core funding No. P1-0222).
commuting graph of a nonabelian finite simple group $A$ is isomorphic to the commuting graph of some group $G$, then groups $A$ and $G$ are isomorphic. In a similar vein, Mohammadian [7] showed that a ring $R$ is isomorphic to the matrix algebra $M_2(F)$ of 2-by-2 matrices over a finite field $F$ if and only if their commuting graphs $\Gamma(R)$ and $\Gamma(M_2(F))$ are isomorphic.

One of the basic questions concerning commuting graphs is their connectedness and diameter. Most of the work that has been done in this regard was the study of the commuting graph of $M_n(F)$, the algebra of $n$-by-$n$ matrices over a field $F$. For example, it is known that its commuting graph is connected if and only if for each field extension $K/F$ of degree $n$, there exists a proper intermediate subfield $F \subseteq L \subseteq K$ (see [1]). Moreover, whenever the commuting graph of $M_n(F)$ is connected, its diameter is bounded above by 6 (see [2]). For a finite field $F$, the commuting graph of $M_n(F)$ has diameter at most 5 if $n$ is neither a prime nor a square of a prime (see [5]). Moreover, its diameter equals exactly 4 in case $n$ is an even number and $n \geq 4$. The diameter of the commuting graph of $M_{p^2}(F)$, $p$ a prime, is (to the author’s knowledge) unsolved as of the writing of this paper.

In this paper, we study the relationship between the structure of a finite ring and the connectivity and diameter of its commuting graph. Since the class of finite rings also includes all the above-mentioned cases of matrix rings over a finite field, the study is of course too broad to be manageable by a single approach. We therefore limit ourselves to special cases, when the structure of the ring is known and manageable enough to provide us with sufficient tools. Thus, we study the diameter of a directly decomposable ring and the connectivity of an indecomposable ring of prime characteristic with the Jacobson radical of nilpotency order 2. The methods we use include the checkered matrix ring over a basic ring associated with the ring in question and a characterization of local rings of prime characteristic with the Jacobson radical of nilpotency order 2.

2. Definitions and preliminaries

Let us recall some basic definitions that we shall use throughout the paper. As usual, in a given graph, the path $a = x_0 - \ldots - x_{i-1} - x_i - \ldots - x_n = b$ connecting vertices $a$ and $b$ has length $n$, and the length of the shortest path connecting vertices $a$ and $b$ is called the distance between $a$ and $b$, and denoted by $d(a, b)$. We denote $d(a, b) = \infty$ if there is no path connecting $a$ and $b$, and we define $d(a, a) = 0$. The diameter of a graph is a maximal distance between any
two of its vertices. Note that the diameter is infinite if there is no finite bound on \(d(a, b)\), where \(a\) and \(b\) range over the vertices.

For a finite ring \(R\), we denote its Jacobson radical by \(J(R)\). The ring \(R\) is called a basic ring or a reduced ring if \(R/J(R)\) is a direct sum of finite fields. We shall denote by \(\mathcal{F} \in R/J\) the image of \(x \in R\) under the canonical homomorphism.

If \(e\) and \(f\) are idempotents in \(R\), we follow [3] and say that \(e\) and \(f\) are isomorphic if \(Re\) and \(Rf\) are isomorphic left \(R\)-modules. If \(ef = fe = f\), we say that \(f \leq e\) and the smallest non-zero idempotent under \(\leq\) is called a minimal idempotent.

Also, we shall denote the diagonal matrix with elements \(a_1, \ldots, a_n\) on the diagonal by \(\text{diag}(a_1, \ldots, a_n)\), and \(E_{ij}\) will denote the matrix with 1 at the position \((i, j)\) and zeros everywhere else.

All rings in this paper are assumed finite and unital, even if this is perhaps not always explicitly stated.

The following lemma is straightforward, but we include the proof for the sake of completeness.

**Lemma 2.1.** Any ring \(R\) can be written as a direct sum of left ideals and each summand is of the form \(Re\), where \(e\) is a minimal idempotent in \(R\).

**Proof.** Let \(S = \{n \in \mathbb{Z}^*; \text{there are distinct nonzero idempotents } e_1, \ldots, e_n \text{ of } R \text{ such that } R = Re_1 \oplus \cdots \oplus Re_n\}\). Observe that \(1 \in S\) (take \(e_1 = 1\)), and also that \(|S| \leq |R|\). Let \(N \in S\) be the largest possible, and let \(e_1, \ldots, e_N\) be distinct nonzero idempotents such that \(R = Re_1 \oplus \cdots \oplus Re_N\). We claim that each \(e_i\) is minimal. Suppose not; without loss of generality, \(e_1\) is not minimal. Thus there is a nonzero idempotent \(f_1 \in R\) such that \(f_1 < e_1\). One shows easily that \(Re_1 = Rf_1 \oplus R(e_1 - f_1)\) and that \(f_1, e_1 - f_1, e_2, \ldots, e_N\) are distinct nonzero idempotents of \(R\) which generate \(R\) as a direct sum. But this yields a contradiction to the maximality of \(N\). \(\Box\)

We can now use this fact in the following definition.

**Definition 2.2.** Suppose \(R\) is a ring and \(R = \oplus_{i=1}^n \oplus_{j=1}^{q_i} L_{ij}^{(j)}\), where \(L_{ij}^{(j)}\) are left ideals such that \(L_{ij}^{(j)}\) is isomorphic to \(L_k^{(i)}\) as a left \(R\)-module if and only if \(i = k\). Denote \(L_{i}^{(j)} = Re_{i}^{(j)}\), where \(\sum_{i=1}^{n} \sum_{j=1}^{q_i} e_{ij}^{(j)} = 1\). Denote \(e_i^{(1)}\) by \(e_i\) for each \(i\) and let \(e = e_1 + e_2 + \cdots + e_n\). We follow [6] to define \(S = eRe\) as the basic ring associated with ring \(R\).

The next short lemma shows that \(S\) is indeed a basic ring, thus the definition makes sense.
Lemma 2.3. The basic ring associated with a ring $R$ is a basic ring.

Proof. Since $e_iSe_j \subseteq S \cap J(R) = J(S)$, we have that $S/J(S) \simeq \oplus_{i=1}^n e_iSe_i$. However, for each $i$, $e_i$ is a minimal idempotent, thus the ring $e_iSe_i$ contains no non-trivial idempotents and is therefore a local ring. But the Jacobson radical of $S/J(S)$ is trivial, so each $e_iSe_i$ is in fact a division ring, and hence a field. □

Let us recall the definition of a checkered matrix ring.

Definition 2.4. Let $R$ be a ring, and $M = \oplus_{i=1}^k M_i$ a direct sum of $R$-modules. Then the ring $\{[\alpha_{ij}] : \alpha_{ij} \in \mathrm{Hom}_R(M_i, M_j)\}$ is called the checkered matrix ring of $M_1, \ldots, M_k$ (and the multiplication of entries is given by the function composition).

Suppose $R = \oplus_{i=1}^n \oplus_{j=1}^q R_{i,j}$, where each $e_i^{(j)}$ is an idempotent and $Re_i^{(j)}$ is isomorphic to $Re_k^{(l)}$ as a left $R$-module if and only if $i = k$. Denote $H_1 = \oplus_{j=1}^q R_{i,j}$ and $e_i = e_i^{(1)}$ for each $i$. We know that $\mathrm{Hom}_R(Re_i, Re_j) \simeq e_iRe_j$ (as abelian groups, see [6, Theorem VII.2]), so one can easily see that $\mathrm{Hom}_R(H_i, H_j)$ is isomorphic as a group to the set of $q_i \times q_j$ matrices with elements in $e_iRe_j$. Thus the checkered matrix ring of $H_1, \ldots, H_n$ is a ring of all block matrices of the form $[A_{ij}]$, where $A_{ij}$ is a $q_i \times q_j$ block matrix with elements in $e_iRe_j$ for the basic ring $S$ associated with $R$. We shall denote this checkered matrix ring by $M(S, \{e_1, e_2, \ldots, e_n\}, \{q_1, q_2, \ldots, q_n\})$.

The following theorem can be found in [6, Theorem X.1].

Theorem 2.5. Let $R$ be a ring. Then there exists a basic ring $S$, a set of orthogonal idempotents $\{e_1, e_2, \ldots, e_n\}$ and a set of positive integers $\{q_1, q_2, \ldots, q_n\}$ such that the ring $R$ is isomorphic to the checkered matrix ring $M(S, \{e_1, e_2, \ldots, e_n\}, \{q_1, q_2, \ldots, q_n\})$.

The next theorem gives us a characterization of local rings of prime characteristic with the Jacobson radical of nilpotency order 2. Its proof can be found in [8, Theorem 3].

Theorem 2.6. Let $R$ be a local ring of prime characteristic $p$ with $J(R) \neq 0$ and $J(R)^2 = 0$. Then there exist integers $n, r, t_2, \ldots, t_n$ such that $R$ is isomorphic to the ring

\[
K(n, r; \ell) := \begin{bmatrix}
    a & b_2 & b_3 & \cdots & b_n \\
    0 & a^{t_2} & 0 & \cdots & 0 \\
    \vdots & \ddots & \ddots & \ddots & \vdots \\
    \vdots & \ddots & a^{t_{n-1}} & 0 & \vdots \\
    0 & 0 & \cdots & 0 & a^{t_n}
\end{bmatrix}; a, b_2, \ldots, b_n \in GF(p^\ell)
\]
where \( k_i = p^{t_i} \) for all \( i = 2, \ldots, n \).

This is now an easy corollary of the theorem.

**Corollary 2.7.** Let \( R \) be a local ring of prime characteristic \( p \) with \( J(R) \neq 0 \), \( J(R)^2 = 0 \) and \( q \geq 2 \). Then there exists a subring \( S \) of \( M_q(R) \) such that \( S \) is isomorphic to \( M_q(R)/J(M_q(R)) \).

**Proof.** Since \( J(M_q(R)) = M_q(J(R)) \), Theorem 2.6 implies that \( J(R) \) consists of all the matrices with zero diagonal, \( S \) is the subring of \( R \) generated by all block matrices such that all their off-diagonal elements are equal to zero. \( \square \)

### 3. The commuting graphs

Let \( R \) be a non-commutative ring, and \( \Gamma = \Gamma(R) \) be its commuting graph. The following lemma shows that in order to study the diameters of commuting graphs of finite rings, we can limit ourselves to directly indecomposable rings.

**Lemma 3.1.** Suppose \( R \) is non-commutative and \( R = R_1 \oplus R_2 \oplus \ldots \oplus R_n \) for some \( n \). Then the following two statements hold:

1. If exactly one of the rings \( R_1, R_2, \ldots, R_n \) is non-commutative (say, \( R_1 \)) then \( \text{diam}(\Gamma(R)) = \text{diam}(\Gamma(R_1)) \).
2. If at least two of the rings \( R_1, R_2, \ldots, R_n \) are non-commutative, then \( \text{diam}(\Gamma(R)) \leq 3 \). In this case, \( \text{diam}(\Gamma(R_i)) \geq 3 \) for all non-commutative rings \( R_i \).

**Proof.** The first statement is obvious. For the second, choose non-central elements \( (a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in R \). Thus, there exist at least one non-central element \( a_i \in R_i \) and at least one non-central element \( b_j \in R_j \). If we can choose any two \( i \neq j \), then there is a path \((a_1, a_2, \ldots, a_n) \to (0, \ldots, 0, a_i, 0, \ldots, 0) \to (0, \ldots, 0, b_j, 0, \ldots, 0) \to (b_1, b_2, \ldots, b_n)\) in \( \Gamma(R) \). Otherwise, the fact that \((b_1, b_2, \ldots, b_n)\) is a non-central element in \( R \) implies that \( b_j \) is non-central in \( R_i \). So, \( a_i, b_i \in R_i \) are non-central elements, and \( a_j, b_j \in R_j \) are central for all \( j \neq i \). By the assumption, there exists \( k \in \{1, 2, \ldots, n\} \) such that \( k \neq i \) and the ring \( R_k \) is non-commutative. Choose a non-central element \( c_k \in R_k \). Now, we have a path \((a_1, a_2, \ldots, a_n) \to (0, \ldots, 0, c_k, 0, \ldots, 0) \to (b_1, b_2, \ldots, b_n)\) in \( \Gamma(R) \). This proves that \( \text{diam}(\Gamma(R)) \leq 3 \).

If there exists \( t \in \{1, \ldots, n\} \) such that \( \text{diam}(\Gamma(R_t)) = 2 \), then, obviously, also \( \text{diam}(\Gamma(R)) = 2 \). Therefore, suppose \( \text{diam}(\Gamma(R_i)) \geq 3 \) for all non-commutative rings \( R_i \). For these \( i \), there exist \( a_i, b_i \in R_i \) that are at distance of at least 3 (and
for all $R_j$ that are commutative choose $a_j = b_j = 0$. Now, examine the elements $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in $R$. If $\text{diam}(\Gamma(R)) = 2$, then $d(a, b) \leq 2$, so there exists at least one $i$ such that $R_i$ is non-commutative and $d(a_i, b_i) \leq 2$, which is a contradiction. \hfill \square

Since every finite ring is uniquely expressible as a direct sum of rings of prime power order (see, for example, [6, Theorem I.1]), we can therefore limit ourselves by the above lemma to studying the commuting graphs of rings of prime power order. As we had previously mentioned, the diameters of commuting graphs of matrix rings over finite fields have been quite heavily studied elsewhere, so here we try to generalize some of those results to the commuting graphs of rings that may have a non-trivial Jacobson radical.

The structure of finite rings in general can still be quite wild, but in some special cases, we can try to characterize the rings in question and then study their commuting graphs. Therefore, we now limit ourselves to rings $R$ of characteristic $p$ with the property that $J(R)^2 = 0$.

The following is our main result.

**Theorem 3.2.** Let $R$ be a non-commutative directly indecomposable ring of prime characteristic $p$ with $J(R)^2 = 0$. Let $\{e_1, \ldots, e_n\}$ be the set of all non-isomorphic minimal idempotents in $R$, and for each $i = 1, \ldots, n$ let $k_i$ denote the number of minimal idempotents in $R$ isomorphic to the idempotent $e_i$. Then the following statements hold:

1. If $n = 1$ and $k_1 = 1$, then $\Gamma(R)$ is not connected.
2. If $n = 1$ and $k_1$ is not a prime, then $\Gamma(R)$ is connected.
3. If $n = 2$ and $k_1 = k_2 = 1$, then $\Gamma(R)$ is not connected.
4. If $n \geq 3$ or $n = 2$ and $k_1 + k_2 \geq 3$, then $\Gamma(R)$ is connected.

**Proof.** If $R = M_k(\mathbb{F})$ for a Galois field $\mathbb{F}$ and $k$ is not prime, then $\Gamma(R)$ is connected by [1, Corollary 7]. Suppose now that $J(R) \neq 0$. By Theorem 2.5, we know that $R$ is isomorphic to $M(S, \{e_1, e_2, \ldots, e_n\}, \{q_1, q_2, \ldots, q_n\})$ for some basic ring $S$, a set of orthogonal idempotents $\{e_1, e_2, \ldots, e_n\}$ and a set of positive integers $\{q_1, q_2, \ldots, q_n\}$. Denote $R = \oplus \sum_{i=1}^{n} \sum_{j=1}^{q_i} Re_i^{(j)}$, where $Re_i^{(j)}$ is isomorphic to $Re_i^{(j)}$ as a left $R$-module if and only if $i = k$. By the proof of [6, Theorem X.1], we know that $S = eRe$ where $e = \sum_{i=1}^{n} e_i^{(1)}$. Since $J(S) = S \cap J(R)$, $S$ is a finite ring of characteristic $p$ with $J(S)^2 = 0$. Also, the fact that $e_i^{(1)}$ is a minimal idempotent implies that the ring $e_i^{(1)}Se_i^{(1)}$ is a local ring with characteristic $p$
and $J \left( e_i^{(1)} S e_i^{(1)} \right)^2 = 0$ for each $i$. This means that for each $i$, either $e_i^{(1)} S e_i^{(1)}$ is a Galois field or $J \left( e_i^{(1)} S e_i^{(1)} \right) \neq 0$. The latter case by Theorem 2.6 implies that $e_i^{(1)} S e_i^{(1)}$ is isomorphic to the ring $K(n_1, r_i; t_{i1})$ for some integers $n_1, r_i$ and some integer $(n_1 - 1)$-tuple $t_{i1}$. If $e_i^{(1)} S e_i^{(1)}$ is a Galois field, we can also assume (by a slight abuse of notation) that $e_i^{(1)} S e_i^{(1)}$ is isomorphic to the ring $K(1, r_i; t_{i1})$ for some integer $r_i$ and an empty set $t_{i1}$. By Theorem 2.5, we know that $R$ is now a block matrix ring, where all the diagonal blocks are matrices from some ring $K(n_1, r_i; t_{i1})$.

Suppose first that $R$ is a local ring (thus $n = 1$ and $R = S = e_1^{(1)} S e_1^{(1)} = K(n_1, r_1; t_{11})$ is a local ring). Since $R$ is not commutative, we have $n_1 \geq 2$ and $r_1 \geq 2$, so there exists $a \in GF(p^n)$ such that $\text{diag}(a, a^{k_2}, \ldots, a^{k_n})$ is a non-central element in $R$ where $k_i = p^{k_i}$ for $i = 2, \ldots, n_1$. However, it can be easily observed that $C_R(\text{diag}(a, a^{k_2}, \ldots, a^{k_n})) = \{ \text{diag}(x, x^{k_2}, \ldots, x^{k_n}); x \in GF(p^n) \}$, so the commuting graph of $R$ is not connected.

Next, examine the case $n = 1$ and $R = M_{q_1}(S)$ with $q_1 \geq 2$. Since $S = e_1^{(1)} S e_1^{(1)}$ and therefore $J(S) \neq 0$, $S$ is a local ring that satisfies the assumptions of Theorem 2.6, so $S = K(n_1, r_1; t_{11})$ with $n_1 \geq 2$. Choose matrices $A, B \in R$ and suppose that $AB = BA$. By Corollary 2.7, there exist matrices $A', B' \in R$ such that $A' B' = B' A'$ with $\overline{A} = \overline{A}$ and $\overline{B} = \overline{B}$. So, $A = A' + j$ for some $j \in J$. We examine two cases: if $B'$ commutes with $j$, then also $A$ commutes with $B'$. So, suppose that $B'$ and $j$ do not commute. Then, since $J^2 = 0$, for any $j' \in J$ we know that $(A' + j)(B' + j') = (B' + j')(A' + j)$ if and only if $A' j' - j' A' = B' j - j B'$. By taking into account the structure of matrices in $R$ by Theorem 2.5, we observe that this is a system of $q_1^2 (q_1 - 1)$ linear equations for $q_1^2 (q_1 - 1)$ variables corresponding to the entries of the matrix $j'$. If this system of linear equations has a maximal rank, then there exists a solution $j' \in J$. If, however, the system does not have a maximal rank, we have a nonzero (and thus noncentral) $j' \in J$ such that $A' j' - j' A' = 0$. This implies that either $A$ commutes with $B' + j'$ or it commutes with $j'$ for some $j' \in J$. Now, choose $C \in R$. Since $R/J = M_{q_1}(F)$ for some Galois field $F$, by [1, Corollary 7] the graph $\Gamma(R/J)$ is connected. Thus, either $\overline{C}$ is central or there either exists a path in $\Gamma(R/J)$ from $\overline{C}$ to the matrix $E_{11}$. By the above argument, this implies that there either exists a path in $\Gamma(R)$ from $C$ to some matrix $j \in J$ or from $C$ to some $D \in R$, such that $\overline{D} = E_{11}$. Since $q_1 \geq 2$, either one of these two matrices commutes with the non-central matrix $x E_{q_1, q_1}$ for some nonzero $x \in J$, which implies that the graph $\Gamma(R)$ is connected.
It remains for us to consider the case $n \geq 2$. Now, for every $i = 1, \ldots, n$, we can see similarly as above that $e_i(1)Se_i(1)$ is either a Galois field or a ring satisfying the assumptions of Theorem 2.6, so $e_i(1)Se_i(1) = K(r_i; t_i)$. Now, each $a \in R$ is of the form $a = a_1 + \cdots + a_n + j$ with $a_i \in e_i(1)Se_i(1)$ for $i = 1, \ldots, n$ and $j \in J$, and if for each $i = 1, \ldots, n$ the element $a_i$ commutes with some element $b_i \in e_i(1)Se_i(1)$, then we can see similarly as above (by observing the system of linear equations for $j'$) that either $a$ commutes with some nonzero element in $J$ or there exists $j' \in J$ such that $a$ commutes with $b_1 + \cdots + b_n + j'$. Suppose first that $n_i \geq 2$ for some $n_i$. Without any loss of generality, we can assume $n_0 = 1$. Then either $a$ commutes with a nonzero element in $J$, or we have an element $j' \in J$ such that $a$ commutes with $b = e_1(1) + j'$, which further commutes with any element in $J(e_1(1)Se_1(1))$. In both cases, we have a path from $a$ to a noncentral element in $J$, which, together with the fact that $J^2 = 0$, implies that the graph $\Gamma(R)$ is connected. Next, examine the case $n_i = 1$ for all $i = 1, \ldots, n$. We have two options: suppose first that $n > 2$. Since $R$ is directly indecomposable, there exist $i \neq j \in \{1, \ldots, n\}$ such that $e_i(1)Se_j(1) \neq 0$. Again, without any loss of generality, we may assume that $i = 1$ and $j = 2$, and choose a nonzero $x \in e_1(1)Se_2(1)$. Choose also an arbitrary noncentral $a \in R$, and with a similar argument as before, proceed to find a path in $\Gamma(R)$ from $a$ either to a noncentral element in $J$ or to some $b = e_1(3) + j'$, where $j' \in J$. However, $b$ then commutes with $x$, so every element is connected with a path to an element in $J$, and since $J^2 = 0$, this shows that $\Gamma(R)$ is a connected graph. Finally, we are left to examine the case $n = 2$ and $k_1 = k_2 = 1$. Choose a nonzero $x \in J$ and notice that the set $\{e_1(1)ae_1(1) + e_2(1)be_2(1) \mid a \neq b \in S\}$ is a connected component of $\Gamma(R)$ that does not include $e_1(1) + e_2(1) + x$, so $\Gamma(R)$ is disconnected. \hfill $\Box$

References


DAVID DOLŽAN
DEPARTMENT OF MATHEMATICS
FACULTY OF MATHEMATICS AND PHYSICS
UNIVERSITY OF LJUBLJANA
JADRANSKA 21
SI-1000 LJUBLJANA
SLOVENIA

E-mail: david.dolzan@fmf.uni-lj.si

(Received July 17, 2018; revised March 14, 2019)