DIAMETERS OF CONNECTED COMPONENTS OF COMMUTING GRAPHS

DAVID DOLŽAN*, MATJAŽ KONVALINKA†, AND POLONA OBLAK†

Abstract. In this paper, we calculate diameters of connected components of commuting graphs of $GL_n(S)$, for an integer $n \geq 2$ and a commutative antinegative entire semiring S, unless n is a non-prime odd number and S has at least two invertible elements.

Key words. Commuting graph, Diameter, Semiring, Symmetric group

AMS subject classifications. 05C50, 20B30

1. Introduction.

A *semiring* is a set S equipped with binary operations $+$ and $\cdot$ such that $(S, +)$ is a commutative monoid with identity element 0, and $(S, \cdot)$ is a monoid with identity element 1. In addition, operations $+$ and $\cdot$ are connected by distributivity and 0 annihilates S. A semiring is *commutative* if $ab = ba$ for all $a, b \in S$.

A semiring S is called *antinegative*, if $a + b = 0$ implies that $a = b = 0$. Antinegative semirings are also called *antirings*. A semiring is said to be *entire* if $ab = 0$ implies that $a = 0$ or $b = 0$. The set of all (multiplicatively) invertible elements of a semiring S will be denoted by $U(S)$. The *centralizer* $C_S(x)$ of $x \in S$ is defined as the set of all elements of S commuting with x.

The simplest example of an antinegative semiring is the *binary Boolean semiring*, the set $\{0, 1\}$ in which addition and multiplication are the same as in $\mathbb{Z}$ except that $1+1 = 1$. Moreover, the set of nonnegative integers (or reals) with the usual operations of addition and multiplication is a commutative antinegative entire semiring. Inclines, additively idempotent semirings in which products are less than or equal to either factor, are commutative antinegative semirings. Distributive lattices are inclines, and thus antinegative semirings. Also, tropical semirings are commutative antinegative semirings.

*Department of Mathematics, University of Ljubljana, Slovenia (david.dolzan@fmf.uni-lj.si, matjaz.konvalinka@fmf.uni-lj.si). Supported by Research Programs P1-0222 and L1-069 of the Slovenian Research Agency

†Department of Computer and Information Science, University of Ljubljana, Slovenia (polona.oblak@fri.uni-lj.si). Supported by Research Program P1-0222 of the Slovenian Research Agency

We will denote by $M_n(S)$ the set of all $n \times n$ matrices over a semiring S and by $GL_n(S)$ the set of all invertible matrices in $M_n(S)$. The symmetric group of permutations on a set of n elements will be denoted by $\mathfrak{S}_n$. A cycle of $\mathfrak{S}_n$ of length n is called a *long cycle*.

The matrix with the only nonzero entry 1 in the ith row and jth column will be denoted by $E_{i,j}$. Let $\operatorname{diag}(a_1, \ldots, a_n)$ denote the diagonal matrix $\sum_{i=1}^n a_i E_{i,i}$. The $n \times n$ identity matrix will be denoted by I_n. For any $\sigma \in \mathfrak{S}_n$ we define the permutation matrix $P_\sigma = \sum_{i=1}^n E_{i,\sigma(i)}$.

For a semigroup G, we denote by $\Gamma(G)$ the *commuting graph* of G. The vertex set $V(\Gamma(G))$ of $\Gamma(G)$ is the set of elements in $G \setminus Z(G)$, where $Z(G) = \{g \in G \colon gh = hg \text{ for all } h \in G\}$ is the centre of G. An unordered pair of vertices $x \sim y$ is an edge of $\Gamma(G)$ if $x \neq y$ and $xy = yx$.

The sequence of edges $x_0 \sim x_1, x_1 \sim x_2, \ldots, x_{k-1} \sim x_k$ is called *a path of length* k and is denoted by $x_0 \sim x_1 \sim \ldots \sim x_k$. The *distance* between two vertices is the length of the shortest path between them. The *diameter* of the graph is the longest distance between any two vertices of the graph.

In [5, Theorem 4], it was shown that the diameter of $\Gamma(\mathfrak{S}_n)$ is 5 for all n except when $n-1$ or n is a prime. Also, by [7, Theorem 3.1], if $n-1$ or n is prime, then $\Gamma(\mathfrak{S}_n)$ is not connected. In [4, Theorem 1], it was shown that if S is a commutative antinegative entire semiring, then $A \in M_n(S)$ is invertible if and only if

$$A = DP_\sigma,$$

where D is an invertible diagonal matrix and P_σ is a permutation matrix.

Recently, the interplay between various algebraic structures and their commuting graphs has been studied, see e.g. [1, 2, 3, 5, 6, 7, 8, 9]. For example, it was recently proved in [8] that a ring is isomorphic to the full matrix ring of 2×2 matrices over a finite field if and only if their commuting graphs are isomorphic. It is conjectured that this is also true for the algebra of $n \times n$ matrices whenever $n \geq 3$. Moreover, the diameters of commuting graphs of rings $M_n(\mathbb{F})$ of $n \times n$ matrices have been studied extensively. It was proved in [1] that if $\mathbb{F}$ is an algebraically closed field and $n \geq 3$, then the diameter of $\Gamma(M_n(\mathbb{F}))$ is always equal to 4. If the field $\mathbb{F}$ is not algebraically closed, then $\Gamma(M_n(\mathbb{F}))$ need not be connected. In the case the graph is connected, its diameter is known to be at most 6 and it is conjectured that it is at most 5. The connectivity and diameters of $\Gamma(GL_n(S))$ were recently studied in [1] for division rings S and in [6] for the ring $S = \mathbb{Z}_m$; that is, the ring of integers modulo m.

In this paper, we calculate diameters of connected components of commuting graphs of $GL_n(S)$ for a commutative antinegative entire semiring S, both when S has only one invertible element, and when it has several such elements. In the first case, it follows from [4, Theorem 1] that $GL_n(S)$ is isomorphic to $\mathfrak{S}_n$. Note that when n is a non-prime odd number and $|U(S)| \geq 2$, we state the diameter as a conjecture.

2. The main result. The purpose of our paper is to prove the following.

THEOREM 2.1. *Let S be a commutative antinegative entire semiring and $n \geq 2$. We have the following table of diameters of connected components of graphs $\Gamma(GL_n(S))$, depending on n and $u = |U(S)|$:*

	$u=1$	$u \geq 2$
$n=2$	(0)	(1^{u+1})
$n=3$	$(1,0^3)$	$(3,1^{u^2})$
$n=4$	$(3,1^4)$	(4)
$n \geq 5, n \in \mathbb{P}$	$(5,1^{(n-2)!})$	$(3,1^{u^{n-1}(n-2)!})$
$n \geq 6, n-1 \in \mathbb{P}$	$(4,1^{n(n-3)!})$	(4)
$n \notin 2\mathbb{N} \cup \mathbb{P}$	(5)	(4) *or* (5)
$n \in 2\mathbb{N}, n-1 \notin \mathbb{P}$	(5)	(4)

Here, $(a_1^{k_1}, \ldots, a_r^{k_r})$ means that the graph has $k_1 + \cdots + k_r$ connected components such that k_i of them have diameter a_i, for $i = 1, \ldots, r$.

REMARK 2.2. *In [5, Theorem 7], the values for $n \geq 4$ even and $u \geq 2$ were erroneously stated to equal* 5*, since Lemma 6, as stated in [5], does not hold. The weaker version of Lemma 6 is about to be published in the errata and proves that there exist two matrices at distance 4, which implies that in the case $u \geq 2$, n not prime and S integral, the diameter of $\Gamma(GL_n(S))$ is either 4 or 5.*

For the proof, we need the following seven propositions. The first one describes the edges in the commuting graph. The next three establish upper bounds for the diameter, and the last three establish lower bounds. Conjecture 2.10 would imply that the diameter of $\Gamma(GL_n(S))$ is 5 if n is odd and non-prime and $u \geq 2$.

PROPOSITION 2.3. *Let $D = \mathrm{diag}(d_1, \ldots, d_n)$ and $E = \mathrm{diag}(e_1, \ldots, e_n)$. In $\Gamma(GL_n(S))$, we have $DP_\alpha \sim EP_\beta$ if and only if $\alpha\beta = \beta\alpha$ and*

$$\frac{d_i}{d_{\beta(i)}} = \frac{e_i}{e_{\alpha(i)}}.$$

PROPOSITION 2.4. *Take $n \geq 4$ even and $u \geq 2$. For every two long cycles $\alpha, \beta \in \mathfrak{S}_n$ and diagonal invertible matrices D and E, the distance in $\Gamma(GL_n(S))$*

between DP_α and EP_β is at most 4.

Proposition 2.5. *Take $n \geq 6$ even with $n-1$ prime and $u = 1$. Then the distance in $\Gamma(GL_n(S))$ between P_α and P_β is at most* 4 *whenever α and β are not cycles of length $n-1$.*

Proposition 2.6. *Let $n \geq 7$ be an odd prime and $u = 1$. Then the distance in $\Gamma(GL_n(S))$ between P_α and P_β is at most* 5 *whenever α and β are not long cycles.*

Proposition 2.7. *[3, Lemma 6.17] Assume that $u = 1$ and n and $n-1$ are not prime. Then the distance in $\Gamma(GL_n(S))$ between P_α and P_β is at least* 5*, where $\alpha = (1, \ldots, n)$ and $\beta = (1, \ldots, n-1)$.*

Proposition 2.8. *Assume that $n = 2m \geq 6$ and $u = 1$. Then the distance in $\Gamma(GL_n(S))$ between P_α and P_β is at least* 4*, where $\alpha = (1, \ldots, 2m)$ and $\beta = (1, m+2, \ldots, 2m, 2, \ldots, m+1)$.*

Proposition 2.9. *Assume that $n = 2m+1 \geq 5$ and $u = 1$. Then the distance in $\Gamma(GL_n(S))$ between P_α and P_β is at least* 5*, where $\alpha = (1, \ldots, 2m)(2m+1)$ and $\beta = (1, ..., m, m+2, ..., 2m+1)(m+1)$.*

Conjecture 2.10. *Assume that $n = 2m+1 \geq 5$ and $u \geq 2$. Then the distance in $\Gamma(GL_n(S))$ between P_α and P_β is at least* 5*, where $\alpha = (1, \ldots, 2m+1)$ and $\beta = (1, \ldots, m, m+2, \ldots, 2m+1, m+1)$.*

Let us see how these propositions prove our main theorem.

Let us start with $n = 2$. For $u = 1$, the graph $\Gamma(GL_2(S))$ consists of a single vertex. If $u \geq 2$, the vertices are $\mathrm{diag}(d_1, d_2)$ for $d_1, d_2 \in U(S)$, $d_1 \neq d_2$, and $\mathrm{diag}(d_1, d_2)P_{(12)}$ for arbitrary $d_1, d_2 \in U(S)$. All diagonal matrices commute with each other. By Proposition 2.3, vertices $\mathrm{diag}(d_1, d_2)$ and $\mathrm{diag}(e_1, e_2)P_{(12)}$ are not connected ($d_1/d_2 = e_1/e_1 = 1$ would imply $d_1 = d_2$), and vertices $\mathrm{diag}(d_1, d_2)P_{(12)}$ and $\mathrm{diag}(e_1, e_2)P_{(12)}$ are connected if and only if $d_1/d_2 = e_1/e_2$. That means that for each $u \in U(S)$, we get a clique of all matrices $\mathrm{diag}(d_1, d_2)P_{(12)}$ with $d_1/d_2 = u$.

Assume $n = 3$. For $u = 1$, the graph $\Gamma(GL_3(S))$ has 5 vertices, corresponding to $\mathfrak{S}_3 \setminus \{\mathrm{id}\}$, and the only edge of the graph connects (123) and (132). If $n = 3$ and $u \geq 2$, then $DP_{(123)}$, where $D = \mathrm{diag}(d_1, d_2, d_3)$, is adjacent to $aDP_{(123)}$ for all $a \in U(S) \setminus \{1\}$, and to $aD'P_{(132)}$, where $a \in U(S)$ and $D' = \mathrm{diag}(d_1d_2, d_2d_3, d_3d_1)$. For every $a, b \in U(S)$, we get a clique that contains $\mathrm{diag}(1, a, b)P_{(123)}$. Furthermore, for every transposition τ, DP_τ is adjacent to some non-scalar diagonal matrix F, and since all diagonal matrices commute, the diameter of this connected component is at most 3. There is no non-scalar diagonal matrix that commutes both with $P_{(12)}$ and $P_{(23)}$, so the diameter equals 3.

If $n = 4$ and $u = 1$, every one of the eight 3-cycles is adjacent only to its inverse. That gives us four 2-cliques. The rest of the graph is shown in Figure 2.1; the large triangle contains (12)(34), (13)(24) and (14)(23). It is obvious that the diameter is 3.

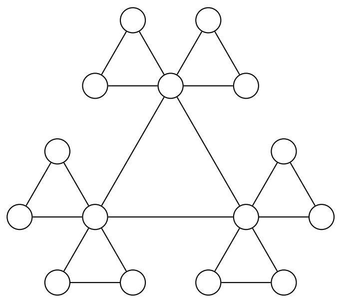

FIG. 2.1. *The large connected component of* $\mathfrak{S}_4$.

For $n = 4$ and $u \geq 2$, every permutation that is not a long cycle is adjacent to a diagonal non-identity matrix: if $T \neq \{1, 2, 3, 4\}$ consists of the elements of some cycle of π, then $DP_\pi \sim \operatorname{diag}(e_1, e_2, e_3, e_4)$, where $e_i = 1$ if $i \in T$ and $e_i = a$ if $i \notin T$, where $a \in U(S) \setminus \{1\}$ is fixed. Since for a long cycle α, we have $DP_\alpha \sim D'P_{\alpha^2} \sim F$ for some D', F, DP_α is at distance at most 4 from EP_β, where β is not a long cycle. By Proposition 2.4, two long cycles are at distance at most 4. That means that the diameter is at most 4. Finally, let us prove that $DP\alpha$ and EP_β are at distance at least 4, where $D = \operatorname{diag}(1, a, a, a)$, $\alpha = (1234)$, $E = \operatorname{diag}(1, 1, a, a)$ and $\beta = (1243)$, where $a \in U(S) \setminus \{1\}$. Then DP_α is adjacent to $D'P_\alpha$ for $D' = b \operatorname{diag}(1, a, a, a)$, where $b \in U(S)$, to $D''P_{\alpha^2}$ for $D'' = b \operatorname{diag}(1, a, a, 1)$, where $b \in U(S)$, and to $D'''P_{\alpha^3}$ for $D''' = b \operatorname{diag}(1, a, 1, 1)$, where $b \in U(S)$. Similarly, EP_β is adjacent to $E'P_\beta$ for $E' = b \operatorname{diag}(1, 1, a, a)$, where $b \in U(S)$, to $E''P_{\beta^2}$ for $E'' = b \operatorname{diag}(1, a, a, a^2)$, where $b \in U(S)$, and to $E'''P_{\beta^3}$ for $E''' = b \operatorname{diag}(1, a, a, 1)$, where $b \in U(S)$. Now α and α^3 do not commute with either β, β^2 or β^3, and β and β^3 do not commute with either α, α^2 or α^3. Furthermore, $D''P_{\alpha^2}$ and $E''P_{\beta^2}$ are not adjacent.

Take $n \geq 5$ prime and $u = 1$. If α is a long cycle, then P_α is adjacent only to P_{α^k} for $k = 2, \ldots, n - 1$. So we get an $(n - 1)$-clique for every long cycle that maps 1 to, say, 2, and there are $(n - 2)!$ such cycles. If $n = 5$, the diameter of the large connected component (with 95 vertices) is easily verified to be 5. For $n \geq 7$, P_α and P_β for α and β that are not long cycles are at distance at most 5 by Proposition 2.6. By Proposition 2.9, the diameter of this connected component is 5.

Suppose that $n \geq 5$ is prime and $u \geq 2$. If α is a long cycle, then DP_α is adjacent to aDP_α for $a \in U(S) \setminus \{1\}$ and to $aD'P_{\alpha^k}$, where $a \in U(S)$, $k = 2, \ldots, n - 1$ and D' is uniquely determined. That means that we get cliques that correspond to DP_α, where $D = \operatorname{diag}(1, a_1, \ldots, a_{n-1})$ and α is a long cycle that maps 1 to 2. So there are $u^{n-1}(n-2)!$ such cliques. For α that is not a long cycle, DP_α commutes with a non-scalar diagonal matrix, and diagonal matrices commute, so the rest of the graph is connected and has diameter at most 3. It is clear that there is no non-scalar diagonal matrix that commutes both with $P_{(1,\ldots,n-1)}$ and $P_{(2,\ldots,n)}$, so the diameter is 3.

Assume that $n \geq 6$, $n-1$ is prime and $u = 1$. Every $(n-1)$-cycle is adjacent only to its powers, so we get cliques corresponding to $(n-1)$-cycles that fix i, $1 \leq i \leq n$, and map, say, the smallest element of $\{1, \ldots, i-1, i+1, \ldots, n\}$ to the second smallest. There are $n(n-3)!$ such cycles. If α, β are not cycles of length $n-1$, the distance between P_α and P_β is at most 4 by Proposition 2.5. By Proposition 2.8, the diameter of the large connected component is 4.

Assume that $n \geq 6$, $n-1$ is prime and $u \geq 2$. For α, β long cycles, the distance between DP_α and EP_β is at most 4 by Proposition 2.4. Also, DP_α is at distance 2 from a non-scalar diagonal matrix. For all other α, DP_α commutes with a non-scalar diagonal matrix. That means that the diameter is at most 4, It is easy to check that $P_{(1,\ldots,n)}$ and $P_{(1,\ldots,n-1)}$ are at distance 4, so the diameter is 4. If $n \geq 6$ is even, $n-1$ is not a prime and $u \geq 2$, the proof that the diameter is 4 is exactly the same.

If $n, n-1$ are not primes and $u = 1$, then we know that $\Gamma(GL_n(S))$ is connected, with diameter at most 5, see [5, Theorem 7(b)]. By Proposition 2.7, the diameter is indeed 5.

Assume that $n \geq 9$ is odd and not prime and $u \geq 2$. Take a long cycle α. For $k|n$, $1 < k < n$, $DP_\alpha \sim D'P_{\alpha^k}$ for some D', and $D'P_{\alpha^k} \sim F$ for some non-scalar diagonal matrix F. If β is not a long cycle, it is adjacent to a non-scalar diagonal matrix. Therefore the graph $\Gamma(GL_n(S))$ is connected with diameter ≤ 5. If $\alpha = (1, \ldots, n)$ and $\beta = (1, \ldots, n-2, n, n-1)$ are different long cycles and $k, l|n$, $k, l \neq n$, then $\beta^l(\alpha^k(n)) = \beta^l(k) = k + l$ and $\alpha^k(\beta^l(n)) = \alpha^k(l-1) = k + l - 1$, so there is no path of length ≤ 3 between P_α and P_β. That means that the diameter is at least 4. If Conjecture 2.10 holds, the diameter is indeed 5.

This completes the proof of the theorem.

3. Proofs of Propositions.

Proof of Proposition 2.3. Write $A = DP_\alpha$, $B = EP_\beta$. Then $(AB)_{ij} = \sum_k a_{ik}b_{kj} = 0$ unless $j = \beta(\alpha(i))$, in which case it is $a_{i\alpha(i)}b_{\alpha(i)\beta(\alpha(i))} = d_i e_{\alpha(i)}$. Similarly, $(BA)_{ij}$ is nonzero (and equal to $e_i d_{\beta(i)}$) if $j = \alpha(\beta(i))$. Therefore DP_α and EP_β are adjacent in $\Gamma(GL_n(S))$ if and only if $\alpha\beta = \beta\alpha$ and $d_i e_{\alpha(i)} = e_i d_{\beta(i)}$.

Proof of Proposition 2.4. Write $n = 2m$.

We claim that there exist diagonal matrices D', E', F and a permutation τ so that

$$DP_\alpha \sim D'P_{\alpha^m} \sim FP_\tau \sim E'P_{\beta^m} \sim EP_\beta,$$

where either $\tau \neq \mathrm{id}$ or $F \neq aI$.

Note that both α^m and β^m are products of m 2-cycles. There are two cases. First, there can be a non-empty proper subset T of $\{1, \ldots, 2m\}$ such that $\alpha^m(T) = \beta^m(T) = T$. In this case, define $F = \mathrm{diag}(f_i)$, where $f_i = 1$ if $i \in T$ and $f_i = a$ if $i \neq T$, where $a \in U(S) \setminus \{1\}$. We have $D'P_{\alpha^m} \sim F \sim E'P_{\beta^m}$ for all D' and E', and by Proposition 2.4 there exist such D' and E' that $DP_\alpha \sim D'P_{\alpha^m}$ and $EP_\beta \sim E'P_{\beta^m}$.

If such a T does not exist, then the set $\{1, \beta^m(1), \alpha^m\beta^m(1), \beta^m\alpha^m\beta^m(1), \ldots\}$, which is obviously non-empty and closed under α^m and β^m, must equal $\{1, \ldots, 2m\}$. That means that

$$\pi = (1, \beta^m(1), \alpha^m\beta^m(1), \beta^m\alpha^m\beta^m(1), \ldots)$$

is a cycle of length $2m$. Define $\tau = \pi^2$. In other words, if $i = (\alpha^m\beta^m)^k(1)$ for some k, then $\tau(i) = \alpha^m\beta^m(i)$, and if $i = \beta^m(\alpha^m\beta^m)^k(1)$ for some k, then $\tau(i) = \beta^m\alpha^m(i)$. Since $m \geq 2$, $\tau \neq \mathrm{id}$.

We claim that $\tau\alpha^m = \alpha^m\tau$. If $i = (\alpha^m\beta^m)^k(1)$ for some k, then $\alpha^m(i) = \beta^m(\alpha^m\beta^m)^{k-1}(1)$ (for $i = 1$, we can take $k = m$), and so $\tau(\alpha^m(i)) = \beta^m\alpha^m(\alpha^m(i)) = \beta^m(i)$. On the other hand, $\tau(i) = \alpha^m\beta^m(i)$, so $\alpha^m(\tau(i)) = \beta^m(i)$. The proof for $i = \beta^m(\alpha^m\beta^m)^k(1)$ for some k is similar, as is the proof that $\tau\beta^m = \beta^m\tau$.

Since $\alpha \sim \alpha^m$, the condition $DP_\alpha \sim D'P_{\alpha^m}$ is equivalent to $d_i/d_{\alpha^m(i)} = d'_i/d'_{\alpha(i)}$. It is easy to see that one set of d'_i's (and the only one up to scalar) that satisfies the equations is

$$d'_i = \prod_{j=0}^{m-1} d_{\alpha^j(i)}.$$

It is clear from these formulas that for every k, $0 \leq k \leq m-1$, we have

$$d'_i d'_{\alpha^m(i)} = d_1 \cdots d_{2m}$$

In other words, $d'_i d'_{\alpha^m(i)}$ is independent of i.

Similarly, up to a scalar, the only solution of $EP_\beta \sim E'P_{\beta^m}$ is

$$e'_i = \prod_{j=0}^{m-1} e_{\beta^j(i)}.$$

and $e'_i e'_{\beta^m(i)}$ is independent of i.

Our goal is to find F so that $D'P_{\alpha^m} \sim FP_\tau \sim E'P_{\beta^m}$. The first condition is equivalent to $d'_i/d'_{\tau(i)} = f_i/f_{\alpha^m(i)}$. Now note that since

$$\frac{d'_i}{d'_{\tau(i)}} \cdot \frac{d'_{\alpha^m(i)}}{d'_{\tau(\alpha^m(i))}} = \frac{d'_i d'_{\alpha^m(i)}}{d'_{\tau(i)} d'_{\alpha^m(\tau(i)))}} = 1,$$

the equations for $f_i/f_{\alpha^m(i)}$ and $f_{\alpha^m(i)}/f_i$ are equivalent. In other words, it is enough that we have

$$\frac{f_i}{f_{\alpha^m(i)}} = \frac{d'_i}{d'_{\tau(i)}} \text{ for } i = (\alpha^m\beta^m)^k(1)$$

and similarly

$$\frac{f_i}{f_{\beta^m(i)}} = \frac{e'_i}{e'_{\tau(i)}} \text{ for } i = \beta^m(\alpha^m\beta^m)^k(1).$$

We have $2m$ equations for f_i's, and each f_i appears exactly once in the numerator and exactly once in the denominator. Furthermore, since $\tau((\alpha^m\beta^m)^k(1)) = (\alpha^m\beta^m)^{k+1}(1)$, the right-hand sides of the first m equations multiply into 1, and similarly the right-hand sides of the second m equations multiply into 1. In other words, these equations have a solution (which is unique up to a scalar factor).

We can even be completely explicit: let us prove that one solution to these equations is

$$f_i = \frac{1}{d'_{\alpha^m\beta^m(i)} e'_{\beta^m(i)}} \text{ if } i = (\alpha^m\beta^m)^k(1),$$

$$f_i = \frac{1}{d'_{\alpha^m(i)} e'_{\beta^m\alpha^m(i)}} \text{ if } i = \beta^m(\alpha^m\beta^m)^k(1).$$

If $i = (\alpha^m\beta^m)^k(1)$ (without loss of generality, $k \geq 1$), then $\alpha^m(i) = \beta^m(\alpha^m\beta^m)^{k-1}(1)$ and $f_{\alpha^m(i)} = (d'_{\alpha^m(\alpha^m(i))} e'_{\beta^m\alpha^m(\alpha^m(i))})^{-1} = (d'_i e'_{\beta^m(i)})^{-1}$ and so

$$\frac{f_i}{f_{\alpha^m(i)}} = \frac{d'_i e'_{\beta^m(i)}}{d'_{\alpha^m\beta^m(i)} e'_{\beta^m(i)}} = \frac{d'_i}{d'_{\tau(i)}}.$$

The proof that $f_i/f_{\beta^m(i)} = e'_i/e'_{\tau(i)}$ for $i = \beta^m(\alpha^m\beta^m)^k(1)$ is completely analogous.

This completes the proof of Proposition 2.4.

EXAMPLE 3.1. *Take $n = 8$, $\alpha = (15386724)$, $\beta = (16823754)$. We have $\alpha^4 = (16)(23)(48)(57)$, $\beta^4 = (13)(24)(58)(67)$, $\pi = (13248576)$ and $\tau = (1287)(3456)$.*
To better understand where τ comes from, let the 2-cycles of α^m and β^m be vertices of a regular octagon so that $(1, \alpha^4(1))$ is the left-most vertex, so that two 2-cycles are adjacent if and only if one of them is a cycle of α^4 and the other one is a cycle of β^4 and they have a common element. Furthermore, choose such an order of the elements of a 2-cycle that neighbours have the common element in the same place.

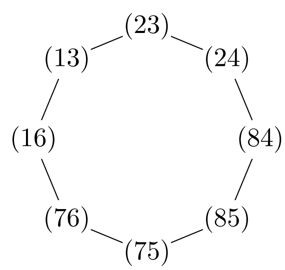

FIG. 3.1. *Constructing τ.*

The first elements of 2-cycles form one cycle of τ (in, say, clockwise direction), and second elements form the other cycle of τ. Clearly, conjugating with τ shifts the 2-cycles clockwise by 2, so both α^4 and β^4 are preserved under conjugation with τ. See Figure 3.1.
We have

$$d'_1 = d_1d_5d_3d_8, \quad d'_5 = d_5d_3d_8d_6, \quad d'_3 = d_3d_8d_6d_7, \quad d'_8 = d_8d_6d_7d_2,$$

$$d'_6 = d_6d_7d_2d_4, \quad d'_7 = d_7d_2d_4d_1, \quad d'_2 = d_2d_4d_1d_5, \quad d'_4 = d_4d_1d_5d_3$$

and similarly

$$e'_1 = e_1e_6e_8e_2, \quad e'_6 = e_6e_8e_2e_3, \quad e'_8 = e_8e_2e_3e_7, \quad e'_2 = e_2e_3e_7e_5,$$

$$e'_3 = e_3e_7e_5e_4, \quad e'_7 = e_7e_5e_4e_1, \quad e'_5 = e_5e_4e_1e_6, \quad e'_4 = e_4e_1e_6e_8.$$

The equations for f_i's (after removing half the equations as described above) are

$$f_1/f_6 = d'_1/d'_2, \quad f_2/f_3 = d'_2/d'_8, \quad f_8/f_4 = d'_8/d'_7, \quad f_7/f_5 = d'_7/d'_1$$

and

$$f_3/f_1 = e_3'/e_4', \quad f_4/f_2 = e_4'/e_5', \quad f_5/f_8 = e_5'/e_6', \quad f_6/f_7 = e_6'/e_3'.$$

If we set $f_1 = (d_2'e_3')^{-1}$*, the only solution is*

$$f_1 = \frac{1}{d_2'e_3'}, \quad f_3 = \frac{1}{d_2'e_4'}, \quad f_2 = \frac{1}{d_8'e_4'}, \quad f_4 = \frac{1}{d_8'e_5'},$$

$$f_8 = \frac{1}{d_7'e_5'}, \quad f_5 = \frac{1}{d_7'e_6'}, \quad f_7 = \frac{1}{d_1'e_6'}, \quad f_6 = \frac{1}{d_1'e_3'}.$$

Proof of Proposition 2.5. Again, write $n = 2m$. Suppose that α and β are long cycles. It is enough to find $\tau \neq \mathrm{id}$ that commutes with α^m and β^m. One such τ is the involution that maps $(\alpha^m\beta^m)^k(1)$ to $(\alpha^m\beta^m)^k\alpha^m(1)$, $(\beta^m\alpha^m)^k\beta^m(1)$ to $(\beta^m\alpha^m)^{k+1}(1)$, and preserves all elements that cannot by reached from 1 by applying α^m and β^m. Compare with the construction of τ in the proof of Proposition 2.4. Then τ is a well-defined involution that commutes with α^m and β^m. We leave the details for the reader.

Assume that neither α nor β is a long cycle. Let us first examine the case where α is a cycle of length less than $n-1$, or α decomposes as a product of disjoint cycles, where at least one cycle has length less than m. Then α commutes with a permutation π with at least $m+1$ fixed points. Now, β either also commutes with a permutation ρ with at least $m+1$ fixed points, in which case π and ρ have a common transposition in their centralizers, or $\beta = \rho_1\rho_2$ is a product of two disjoint m-cycles. In the latter case, β commutes with both ρ_1 and ρ_2 and we can choose the one that has more of its fixed points in common with π. If α and β are both products of two disjoint m-cycles, we can also always choose one m-cycle from each permutation such that they have at least two common fixed points and therefore a common transposition in their centralizers.

Let α be a long cycle. If $\beta = \rho_1 \dots \rho_r$, where there exists i such that the length of ρ_i is at least 2 and at most $m-1$, then β commutes with ρ_i which has at least $m+1$ fixed points. Thus, ρ_i commutes with at least one transposition in the cyclic decomposition of α^m. Suppose now $\beta = \rho_1\rho_2$ is a product of two m-cycles. If the cycle ρ_j is disjoint from some transposition τ in the cyclic decomposition of α^m, then $\alpha \sim \alpha^m \sim \tau \sim \rho_j \sim \beta$ is a path in $\Gamma(GL_n(S))$, thus the distance between α and β is at most 4. Otherwise, each transposition in the cyclic decomposition of α^m has one element from $\rho_1 = (a_1, \dots, a_m)$ and one element from $\rho_2 = (b_1, \dots, b_m)$. We can assume that $\tau = (a_1, b_1)$ is a transposition in the cyclic decomposition of α^m, since we can cyclically permute the elements of ρ_2. Now, $\beta \sim (a_1, b_1) \cdots (a_m, b_m) \sim$

$\tau \sim \alpha^m \sim \alpha$ is a path of length 4 in $\Gamma(GL_n(S))$ between α and β. It only remains to show that α and $\beta = \rho_1$ are also at distance at most 4, where ρ_1 is a cycle of length at most $n-2$. In this case, β has at least 2 fixed points, say b_1, b_2, so it commutes with the transposition $\tau = (b_1, b_2)$. Since τ has $n-2 > m$ fixed points, it commutes with at least one transposition σ in the cyclic decomposition of α^m. Therefore, $\alpha \sim \alpha^m \sim \sigma \sim \tau \sim \beta$ is a path of length 4 in $\Gamma(GL_n(S))$ between α and β.

Proof of Proposition 2.6. Since n is prime, we can write $n = 2m+1$, where $m \geq 3$. Assume first that α is a cycle. If α is a cycle of length $n-1$, then α^m is a product of m disjoint transpositions, therefore α is at distance 2 to the disjoint transpositions $\pi_1, \ldots, \pi_m$. If α is a cycle of length less than $n-1$, then α commutes with at least one transposition (consisting of two fixed points of α), so α is also at distance 2 to at least m disjoint transpositions. Now, if β is also a cycle, we can similarly see that it is at distance 2 to m disjoint transpositions $\rho_1, \ldots, \rho_m$, but since $m \geq 3$ there exist i and j such that π_i and ρ_j are disjoint and therefore commute, proving that α and β are at distance 5 or less. Otherwise, we have a decomposition $\beta = \rho_1 \cdots \rho_r$ into a product of disjoint cycles of increasing length. Note that the length of ρ_1 has to be at most m, so ρ_1 commutes with every transposition with elements from the set of at least $m+1 \geq 4$ elements, so one of these transpositions has to be disjoint with, say, π_1. Now, the only remaining case is when neither α nor β are cycles. But then both α and β are at distance two to a set of all transpositions consisting of elements from some sets of size at least 4, so we can always choose two disjoint transpositions that commute, which proves that α and β are indeed at distance 5 or less.

Proof of Proposition 2.8. Suppose otherwise, *i.e.* there exists a path $\alpha \sim \alpha^k \sim \beta^l \sim \beta$ in $\Gamma(GL_n(S))$ for some integers $1 \leq k, l \leq 2m$. Since commuting with a permutation is equivalent to commuting with its inverse, we can suppose that $1 \leq k, l \leq m$. So,

$$\alpha^k \beta^l(1) = \begin{cases} m+l+k+1 \pmod{2m}, & l \leq m-1 \\ k+2, & l = m. \end{cases}$$

Since α^k and β^l commute, we have that $\alpha^k\beta^l(1) = \beta^l\alpha^k(1)$. If $l \leq m-1$, we have

$$m+l+k+1 \pmod{2m} = \beta^l\alpha^k(1) = \beta^l(k+1) = \begin{cases} k+l+1, & l \leq m-k \\ 1, & l = m-k+1 \\ k+l, & m-k+2 \leq l \leq m-1, \end{cases}$$

a contradiction. In the latter case, $l = m$, we obtain that

$$k+2 = \beta^m \alpha^k(1) = \beta^m(k+1) = \begin{cases} k+m & k>1 \\ 1 & k=1 \end{cases},$$

which is again a contradiction.

Proof of Proposition 2.9. We have to prove that there is no path of length 4 or less between α and β. Note that α and β commute only with the powers of themselves, so suppose there exists γ such that γ commutes with α^k and β^l for some k and l. First, we prove that we can assume that k divides $2m$. Let $d = \gcd(k, 2m)$. Let s and t be integers such that $ks + 2mt = d$. Since $\alpha \sim \alpha^k \sim \gamma$ is a path in $\Gamma(\mathfrak{S}_n)$, $\alpha \sim \alpha^{sk} \sim \gamma$ is also a path in $\Gamma(\mathfrak{S}_n)$. Since $\alpha^{sk} = \alpha^{d(1-2mt)} = \alpha^d(\alpha^{2m})^{-t} = \alpha^d$, $\alpha \sim \alpha^d \sim \gamma$ is a path in $\Gamma(\mathfrak{S}_n)$. We can similarly assume that l divides $2m$.

Suppose first that $k \le l$. Since $2m+1$ is the only fixed point of the permutation α^k and $\alpha^k(\gamma(2m+1)) = \gamma(\alpha^k(2m+1)) = \gamma(2m+1)$, we see that $2m+1$ is also a fixed point of γ. Similarly, $m+1$ is a fixed point of β and thus also a fixed point of γ.

If $f \le m$ is a fixed point for γ, then by applying α^{ak} for a suitable integer a, we can achieve that $f+ak$, $1 \le f+ak \le m$, is also a fixed point of γ. We can choose a such that $f+ak \le m$ and $f+(a+1)k > m$. This implies that $\beta^l(f+ak) = f+ak+l+1$ is also a fixed point for γ. But similarly, for any fixed point $f \ge m$ we can choose b such that $f+bk \le 2m+1$ and $f+(b+1)k > 2m+1$, so $\beta^l(f+bk) = f+bk+l-2m-1$ is also a fixed point for γ. Since we can repeat either of these two steps arbitrarily many times, by also applying α^k (and thus getting rid of $2m$, ak and bk), we arrive at the conclusion that $f + c(l+1) + d(l-1)$ is a fixed point for γ for any c and d.

If l is even, this implies that γ is an identity. If l is odd, all odd numbers are fixed points for γ, since $\beta^l(2m+1) = l$ is a fixed point. If m is odd, all even numbers are also fixed points, since $m+1$ is an even fixed point for γ. On the other hand, if m is even, then $l < m$ and $\beta^l(1) = l+1$ is an even fixed point.

Let us now look at the case $l < k$. Since α^k commutes with γ and γ commutes with β^l, for each τ also $(\tau\alpha\tau^{-1})^k$ commutes with $\gamma' = \tau\gamma\tau^{-1}$ and γ' commutes with $(\tau\beta\tau^{-1})^l$. If we choose $\tau = (m+1, \ldots, 2m+1)$, we get $\alpha' = \tau\alpha\tau^{-1} = (1, \ldots, m, 2m+1, m+1, \ldots, 2m-1)(2m)$ and $\beta' = \tau\beta\tau^{-1} = (1, \ldots, 2m)(2m+1)$. We can now proceed similarly as above. Namely, let $f \le m$ be a fixed point for γ'. By applying β'^{al} for a suitable integer a, we can achieve that $f+al$, $1 \le f+al \le m$, is also a fixed point of γ'. We can choose a such that $f+al \le m$ and $f+(a+1)l > m$. This implies that $\alpha'^k(f+al) = f+al+k-1$ (since $k > l$, $\alpha'^k(f+al) \ne 2m+1$) is also a fixed point for γ'. But similarly, for any fixed point $f \ge m$ we can choose b such that

$f+bl \leq 2m$ and $f+(b+1)l > 2m$, so $\alpha'^k(f+bl) = f+bl+k+1-2m$ is also a fixed point for γ'. Since we can repeat either of these two steps arbitrarily many times, by also applying β^l (and thus getting rid of $2m$, al and bl), we arrive at the conclusion that $f+c(k+1)+d(k-1)$ is a fixed point for γ' for any c and d. But since both $2m$ and $2m+1$ are fixed points for γ', γ' has to be an identity.

REFERENCES

[1] S. Akbari, A. Mohammadian, H. Radjavi, and P. Raja. On the diameters of commuting graphs. *Linear Algebra Appl.*, 418(1):161–176, 2006.

[2] S. Akbari and P. Raja. Commuting graphs of some subsets in simple rings. *Linear Algebra Appl.*, 416(2-3):1038–1047, 2006.

[3] J. Araújo, W. Bentz, and J. Konieczny. The commuting graph of the symmetric inverse semigroup. arXiv:1205.1664, May 2012.

[4] D. Dolžan and P. Oblak. Invertible and nilpotent matrices over antirings. *Linear Algebra Appl.*, 430(1):271–278, 2009.

[5] D. Dolžan and P. Oblak. Commuting graphs of matrices over semirings. *Linear Algebra Appl.*, 435(7):1657–1665, 2011.

[6] M. Giudici and A. Pope. The diameters of commuting graphs of linear groups and matrix rings over the integers modulo m. *Australas. J. Combin.*, 48:221–230, 2010.

[7] A. Iranmanesh and A. Jafarzadeh. On the commuting graph associated with the symmetric and alternating groups. *J. Algebra Appl.*, 7(1):129–146, 2008.

[8] A. Mohammadian. On commuting graphs of finite matrix rings. *Comm. Algebra*, 38(3):988–994, 2010.

[9] Y. Segev. The commuting graph of minimal nonsolvable groups. *Geom. Dedicata*, 88(1-3):55–66, 2001.