THE CRITICAL GROUPS OF THE PEISERT GRAPHS

PETER SIN

Abstract. The critical group of a finite graph is an abelian group defined by the Smith normal form of the Laplacian. We determine the critical groups of the Peisert graphs, a certain family of strongly regular graphs similar to, but different from, the Paley graphs. It is further shown that the adjacency matrices of the two graphs defined over a field of order p^2 with $p \equiv 3 \pmod 4$ are similar over the ℓ-local integers for every prime ℓ. Consequently, each such pair of graphs provides an example where all the corresponding generalized adjacency matrices are both cospectral and equivalent in the sense of Smith normal form.

1. Introduction

Let $\Gamma = (V, E)$ be a finite, simple, undirected and connected graph and let A be the adjacency matrix of Γ with respect to some fixed but arbitrary ordering of the vertex set V of Γ. Let D be the diagonal matrix whose (i,i)-entry is the degree of the i^{th} vertex. Then $L = D - A$ is called the *Laplacian matrix* of Γ. The matrices A and L represent endomorphisms (which will also be denoted by A and L) of the free abelian group on V. The structure of their cokernels as abelian groups is independent of the above ordering and can be found by computing the Smith normal forms of the matrices. The cokernel of A is called the *Smith group*. The endomorphism L maps the sum of all vertices to zero, so its cokernel is not a torsion group. The torsion subgroup $K(\Gamma)$ of the cokernel of L is called the *critical group* of Γ. It is known by Kirchhoff's matrix-tree theorem that the order of $K(\Gamma)$ is equal to the number of spanning trees of Γ.

One source of motivation for the study of the critical group came from physics [7], where it was called the *sandpile group*. In graph theory an early author on the critical group was Vince [20], who computed them for wheels and complete bipartite graphs, and pointed out that the critical group depends only on the cycle matroid of the graph. Other papers containing calculations of critical groups for families of graphs include Bai [1], Jacobson [11], Jacobson-Niedermaier-Reiner [12], Ducey-Jalil [8] and Chandler-Sin-Xiang [5]. Lorenzini [13] has examined the proportion of graphs with cyclic critical groups among graphs having critical groups of a particular order, while Wood [22] has determined the distribution of the critical groups of the Erdös-Rényi random graphs.

The object of the present paper is to add one more family to the class of computed examples, by applying some of the ideas used for Paley graphs in [5] to the Peisert graphs. We shall obtain a complete description of the group structure of the critical groups of the Peisert graphs. However, unlike in [5], we are not able to obtain a neat description of the generating function for the multiplicities of elementary divisors, so in this sense the results are less satisfactory.

This work was partially supported by a grant from the Simons Foundation (#204181 to Peter Sin).

Part of this work was done during a visit to the Institute for Mathematical Sciences, Natonal University of Singapore in 2016 for the program: New Directions in Combinatorics.

In the final section we study more closely the Peisert graphs and Paley graphs defined over the field of p^2 elements. Suppose A is the adjacency matrix of a graph on n vertices and let I denote the $n \times n$ identity matrix and J the $n \times n$ matrix whose entries are all equal to 1. Then the *generalized adjacency matrices* are the matrices $aA + bI + cJ$ for integers a, b and c. Among the generalized adjacency matrices are the Seidel $(-1, 0, 1)$ adjacency matrix, the adjacency matrix of the complementary graph and, in the case of a regular graph, the Laplacian and signless Laplacian matrices, We show that, when $q = p^2$, each generalized adjacency matrix of the Peisert graph is cospectral with, and has the same Smith normal form as, the corresponding generalized adjacency matrix of the Paley graph. These properties are derived from the stronger property that the adjacency matrices are similar by an invertible matrix over a ring of algebraic integers.

2. Definitions and notation

2.1. **The Peisert graphs.** Here, we describe the family of graphs $P^*(q)$ constructed in [16]. Let $q = p^{2t}$, for a prime p with $p \equiv 3 \pmod 4$, and t a positive integer. Let β be a primitive element in $\mathbb{F}_q$. In the multiplicative group $\mathbb{F}_q^\times$, the subgroup C_0 of nonzero 4-th powers has index 4. Let C_1 be the coset βC_0 and let $S' = C_0 \cup C_1$. The graph $P^*(q)$ has vertex set $\mathbb{F}_q$, with two vertices x and y joined by an edge if and only if $x - y \in S'$. As observed in [16] the isomorphism type of $P^*(q)$ does not depend on the choice of β. The graphs $P^*(q)$ and the Paley graphs Paley(q) ([4, p.101]) are both Cayley graphs on an elementary abelian group of order q and are cospectral, but not isomorphic except when $q = 9$ ([16, §6]).

Thus, the graphs $P^*(q)$ form an infinite family of self-complementary strongly regular graphs (also known as *conference graphs*) of non-Paley type. There are many ways to construct graphs with the same parameters that are Cayley graphs on the same group. (See [15], [21].) The aim of this paper is to compute certain matrix invariants of the graphs $P^*(q)$, in particular their *critical groups*.

2.2. **The Smith group and the critical group.** Let R be a principal ideal domain. Then the matrix version of the fundamental theorem on finitely generated R-modules says that every $m \times n$ matrix X over R is *R-equivalent* to its *Smith normal form*. That is to say, there exist an $m \times m$ matrix P and an $n \times n$ matrix Q, both invertible over R, such that $PXQ = D$, where

$$D = \begin{bmatrix} D_1 & 0 \\ 0 & 0 \end{bmatrix}$$

with $D_1 = \mathrm{diag}(s_1, s_2, \ldots, s_r)$, $s_1 \mid s_2 \mid \cdots \mid s_r$, and $r = \mathrm{rank}\, X$. If we consider the R-module homomorphism $\mu_X : R^n \to R^m$ given by left multiplication by X, then the Smith normal form describes the decomposition of $\mathrm{coker}(\mu_X)$, called the *Smith group* of X, into cyclic R-submodules. Sometimes, it is convenient to drop the divisibility requirement and work with other "diagonal forms" of X, which also determine the Smith group.

Given a finite graph $\Gamma = (V, E)$, with V ordered in some way, two important integer matrices are the adjacency matrix A and the Laplacian matrix L. If we take $R = \mathbb{Z}$ then, as already stated in the Introduction, the *Smith group of* Γ is defined to be the Smith group of A and the *critical group of* Γ is defined to be the torsion subgroup of the Smith group of L . We shall denote the critical group of Γ by $K(\Gamma)$.

3. The Smith group and the p'-torsion of the critical group of $P^*(q)$

$P^*(q)$ is a strongly regular graph, cospectral with Paley(q). The eigenvalues of its adjacency matrix are $\frac{q-1}{2}$, $\frac{-1+\sqrt{q}}{2}$ and $\frac{-1-\sqrt{q}}{2}$, with multiplicities 1, $\frac{q-1}{2}$ and $\frac{q-1}{2}$, respectively. (See, for example, [8.1.1][4]). Since the order of the critical group is determined by the spectrum we have $|K(P^*(q))| = |K(\text{Paley}(q))|$. In [5, §2] it was shown that the isomorphism type of the Smith group $S(\text{Paley}(q))$ and that of the p-complementary part $K(\text{Paley}(q))_{p'}$ of the critical group could also be determined from the spectrum and the property of being a Cayley graph on an elementary abelian group of order q. The same argument applies to the p-complementary part of the Smith group of all the matrices $A+cI$, where A is the adjacency matrix and c is an integer. In particular, for $P^*(q)$, or indeed any cospectral Cayley graph on an elementary abelian group of order q, these groups are isomorphic to the corresponding groups for Paley(q). Thus, we have the following results.

Theorem 3.1. *The Smith group of $P^*(q)$ is isomorphic to $\mathbb{Z}/2r\mathbb{Z}\oplus(\mathbb{Z}/r\mathbb{Z})^{2r}$, where $r = \frac{q-1}{4}$.*

Theorem 3.2. *Let $K(P^*(q)) = K(P^*(q))_p \oplus K(P^*(q))_{p'}$ be the decomposition of the critical group of $P^*(q)$ into its Sylow p-subgroup and p-complement. Then $K(P^*(q))_{p'} \cong (\mathbb{Z}/r\mathbb{Z})^{2r}$, where $r = \frac{q-1}{4}$. The order of $K(P^*(q))_p$ is equal to $q^{\frac{q-3}{2}}$.*

Later, we shall see that the critical groups of the Paley graphs and Peisert graphs for the same q are generally not isomorphic, although they are isomorphic when $q = p^2$.

4. The Sylow p-subgroup of the critical group

We are left with the problem of determining the cyclic decomposition of the Sylow p-subgroup of $K(P^*(q))$ or, in other words, the p-elementary divisors of L.

Let $R_0 = \mathbb{Z}[\xi]$, where ξ is a primitive $(q-1)$-st root of unity in an algebraic closure of $\mathbb{Q}$, and let π be a prime ideal of R_0 containing p. As p is unramified in R_0, in the localization $R = (R_0)_\pi$, the ideal pR is a maximal with $R/pR \cong \mathbb{F}_q$. We denote by $v_p(a)$ the p-adic valuation of an element $a \in R$. Let $R^{\mathbb{F}_q}$ be the free R-module with basis indexed by $\mathbb{F}_q$. For clarity, we write the basis element corresponding to $x \in \mathbb{F}_q$ as $[x]$.

Let $T : \mathbb{F}_q^\times \to R^\times$, $T(\beta^j) = \xi^j$, be the Teichmüller character, which generates the cyclic group $\text{Hom}(\mathbb{F}_q^\times, R^\times)$.

Then $\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q}$, which decomposes as the direct sum $R[0] \oplus R^{\mathbb{F}_q^\times}$, and $R^{\mathbb{F}_q^\times}$ decomposes further into the direct sum of $\mathbb{F}_q^\times$-invariant components of rank 1, affording the characters T^i, $i = 0,\ldots,q-2$. The component affording T^i is spanned by

$$e_i = \sum_{x \in \mathbb{F}_q^\times} T^i(x^{-1})[x].$$

Here the subscript i is read modulo $q-1$. So $R^{\mathbb{F}_q}$ has basis $\{e_i \mid i = 1,\ldots q-2\} \cup \{e_0, [0]\}$, where we have separated out the basis for the $\mathbb{F}_q^\times$-fixed points.

Next consider the action of the subgroup C_0. The characters T^i,T^{i+r},T^{i+2r}, and T^{i+3r} are equal when restricted to C_0 and for $i \notin \{0, r, 2r, 3r\}$ the elements e_i, e_{i+r}, e_{i+2r} and e_{i+3r} form a basis for the C_0-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in C_0\}$$

of $R^{\mathbb{F}_q}$ for $1 \le i \le \frac{q-5}{4}$. In addition we denote by M_0 the isotypic component of the principal character of C_0, namely the submodule of C_0-fixed points in $R^{\mathbb{F}_q}$. As a basis for M_0, we take

$\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0]$, $[0]$, e_r, e_{2r} and e_{3r}. Thus,

$$R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i. \tag{1}$$

Since μ_L is an RC_0-module homomorphism, it maps each summand into itself, and so with respect to the basis formed from the above bases of the M_i, the matrix of μ_L is block-diagonal with $\frac{q-5}{4}$ 4×4 blocks and a single 5×5 block. Next we compute these blocks. In these computations, Jacobi sums will arise, so we recall their definition.

Definition 4.1. Let θ and ψ be multiplicative characters of $\mathbb{F}_q^\times$ taking values in $R^\times$. By convention, we extend the domain of characters to $\mathbb{F}_q$ by setting the value of the principal character at 0 to be 1, while nonprincipal characters are assigned the value 0 there. The *Jacobi sum* is

$$J(\theta, \psi) = \sum_{x \in \mathbb{F}_q} \theta(x)\psi(1-x). \tag{2}$$

We refer to [3, Ch. 2] for the elementary formal properties of Jacobi sums. At this point we fix some notation for the rest of the paper. Let $r = \frac{(q-1)}{4}$, $\eta = \xi^r$, $\alpha = \frac{(1-\eta)}{2}$ and $\overline{\alpha} = \frac{(1+\eta)}{2}$. Then the characteristic function of S' is

$$\delta_{S'} = \frac{1}{2}(T^0 - \delta_0 + \alpha T^r + \overline{\alpha} T^{-r}), \tag{3}$$

where δ_0 takes the value 1 at 0 and 0 on $\mathbb{F}_q^\times$ and (by our convention) the principal character T^0 sends all elements of $\mathbb{F}_q$ to 1. We also note for later use that since $q \equiv 1 \pmod 8$, we have $T^r(-1) = 1$.

Lemma 4.2. *Suppose $i \notin \{0, r, 3r\}$. Then*

$$\mu_L(e_i) = \frac{1}{2}(qe_i - \overline{\alpha} J(T^{-i}, T^{-r}) e_{i+r} - \alpha J(T^{-i}, T^{-3r}) e_{i+3r}).$$

Proof. Since $L = (\frac{q-1}{2})I - A$, we will work with A. By definition of A, we have

$$\begin{aligned}
2\mu_A(e_i) &= 2 \sum_{x \in \mathbb{F}_q^\times} T^{-i}(x) \sum_{y \in \mathbb{F}_q} \delta_{S'}(y)[x+y] \\
&= \sum_{x \in \mathbb{F}_q^\times} T^{-i}(x) \sum_{y \in \mathbb{F}_q} (T^0(y) - \delta_0(y) + \alpha T^r(y) + \overline{\alpha} T^{-r}(y))[x+y] \\
&= \sum_{x \in \mathbb{F}_q^\times} T^{-i}(x) \sum_{y \in \mathbb{F}_q} [x+y] - \sum_{x \in \mathbb{F}_q^\times} T^{-i}(x)[x] \\
&\quad + \alpha \sum_{x \in \mathbb{F}_q^\times} T^{-i}(x) \sum_{y \in \mathbb{F}_q} T^r(y)[x+y] + \overline{\alpha} \sum_{x \in \mathbb{F}_q^\times} T^{-i}(x) \sum_{y \in \mathbb{F}_q} T^{-r}(y)[x+y] \\
&= 0 - e_i + \alpha\sigma + \overline{\alpha}\sigma',
\end{aligned}$$

where

$$\sigma = \sum_{x \in \mathbb{F}_q^\times} T^{-i}(x) \sum_{y \in \mathbb{F}_q} T^r(y)[x+y] \quad \text{and} \quad \sigma' = \sum_{x \in \mathbb{F}_q^\times} T^{-i}(x) \sum_{y \in \mathbb{F}_q} T^{-r}(y)[x+y].$$

Then, by substituting $z = x + y$ and changing the order of summation, we have

$$\begin{aligned}\sigma &= \sum_{z\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q^\times} T^{-i}(x)T^r(z-x)[z] \\ &= \sum_{z\in\mathbb{F}_q^\times}\sum_{x\in\mathbb{F}_q^\times} T^{-i}(x)T^r(z-x)[z],\end{aligned}$$

as the inner sum vanishes for $z = 0$, by the orthogonality of characters. Then as

$$T^{-i}(x)T^r(z-x) = T^{-i}(x/z)T^r(1-x/z)T^{-i+r}(z)$$

we obtain

$$\sigma = J(T^{-i}, T^{-3r})e_{i+3r}.$$

Similarly, $\sigma' = J(T^{-i}, T^{-r})e_{i+r}$. □

Lemma 4.3. (i) $\mu_L(\mathbf{1}) = 0$.
(ii) $\mu_L([0]) = \frac{1}{2}(-\mathbf{1} + q[0] - \overline{\alpha}e_r - \alpha e_{3r})$.
(iii) $\mu_L(e_r) = \frac{1}{2}(\alpha\mathbf{1} - q\alpha[0] + qe_r - \overline{\alpha}J(T^{-r}, T^{-r})e_{2r})$.
(iv) $\mu_L(e_{2r}) = \frac{1}{2}(-\alpha J(T^{-2r}, T^{-3r})e_r + qe_{2r} - \overline{\alpha}J(T^{-2r}, T^{-r})e_{3r})$.
(v) $\mu_L(e_{3r}) = \frac{1}{2}(\overline{\alpha}\mathbf{1} - q\overline{\alpha}[0] - \alpha J(T^{-3r}, T^{-3r})e_{2r} + qe_{3r})$.

Proof. As $L = (\frac{q-1}{2})I - A$, it is enough to compute $2\mu_A$ on the basis elements. Part (i) is obvious. For (ii) we have

$$\begin{aligned}2\mu_A([0]) &= 2\sum_{y\in\mathbb{F}_q}\chi_{S'}(y)[y] \\ &= \mathbf{1} - [0] + \alpha\sum_{y\in\mathbb{F}_q} T^{-3r}(y)[y] + \overline{\alpha}\sum_{y\in\mathbb{F}_q} T^{-r}(y)[y] \\ &= \mathbf{1} - [0] + \alpha e_{3r} + \overline{\alpha}e_r.\end{aligned}$$

Part (iv) is the case $i = 2r$ of Lemma 4.2. It remains to prove (iii) and (v). It suffices to prove (iii) since the two cases are related by an automorphism of $\mathbb{F}_q$. By definition of A, we have

$$\begin{aligned}2\mu_A(e_r) &= 2\sum_{x\in\mathbb{F}_q^\times} T^{-r}(x)\sum_{y\in\mathbb{F}_q}\delta_{S'}(y)[x+y] \\ &= \sum_{x\in\mathbb{F}_q^\times} T^{-r}(x)\sum_{y\in\mathbb{F}_q}(T^0(y) - \delta_0(y) + \alpha T^r(y) + \overline{\alpha}T^{-r}(y))[x+y] \\ &= \sum_{x\in\mathbb{F}_q^\times} T^{-r}(x)\sum_{y\in\mathbb{F}_q}[x+y] - \sum_{x\in\mathbb{F}_q^\times} T^{-r}(x)[x] \\ &\quad + \alpha\sum_{x\in\mathbb{F}_q^\times} T^{-r}(x)\sum_{y\in\mathbb{F}_q} T^r(y)[x+y] + \overline{\alpha}\sum_{x\in\mathbb{F}_q^\times} T^{-r}(x)\sum_{y\in\mathbb{F}_q} T^{-r}(y)[x+y] \\ &= 0 - e_r + \alpha\sigma + \overline{\alpha}\sigma',\end{aligned}$$

where

$$\sigma = \sum_{x\in\mathbb{F}_q^\times} T^{-r}(x)\sum_{y\in\mathbb{F}_q} T^r(y)[x+y] \quad \text{and} \quad \sigma' = \sum_{x\in\mathbb{F}_q^\times} T^{-r}(x)\sum_{y\in\mathbb{F}_q} T^{-r}(y)[x+y].$$

Then, by substituting $z = x + y$ and changing the order of summation, we have

$$\begin{aligned}\sigma &= \sum_{z\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q^\times} T^{-r}(x)T^r(z-x)[z]\\ &= (q-1)[0] + \sum_{z\in\mathbb{F}_q^\times}\sum_{x\in\mathbb{F}_q^\times} T^{-r}(x)T^r(z-x)[z],\end{aligned}$$

as the inner sum when $z = 0$ is $(q-1)[0]$.

For $z \neq 0$ we have

$$T^{-r}(x)T^r(z-x) = T^{-r}(x/z)T^r(1-x/z)T^{-4r}(z)$$

and so

$$\sum_{x\in\mathbb{F}_q^\times} T^{-r}(x/z)T^r(1-x/z)T^{-4r}(z) = J(T^{-r},T^r)[z] = -T^r(-1)[z] = -[z]$$

So

$$\sum_{z\in\mathbb{F}_q^\times}\sum_{x\in\mathbb{F}_q^\times} T^{-r}(x)T^r(z-x)[z] = -(\mathbf{1}-[0]).$$

Thus, $\sigma = q[0] - \mathbf{1}$. We now turn to σ'. By substituting $z = x + y$ and changing the order of summation, we have

$$\begin{aligned}\sigma' &= \sum_{z\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q^\times} T^{-r}(x)T^{-r}(z-x)[z]\\ &= \sum_{z\in\mathbb{F}_q^\times}\sum_{x\in\mathbb{F}_q^\times} T^{-r}(x)T^{-r}(z-x)[z],\end{aligned}$$

as the inner sum when $z = 0$ is 0. For $z \neq 0$ we have

$$T^{-r}(x)T^{-r}(z-x) = T^{-r}(x/z)T^{-r}(1-x/z)T^{-2r}(z),$$

and so

$$\sigma' = J(T^{-r},T^{-r})e_{2r}.$$

□

An integer j which is not divisible by $q-1$ has, when reduced modulo $q-1$, a unique p-digit expression $j = a_0 + a_1p + a_2p^2 + \cdots + a_{2t-1}p^{2t-1}$, where $0 \le a_i \le p-1$. We shall write this p-digit expression a $2t$-tuple $(a_0, a_1, \ldots, a_{2t-1})$. Let $s(j)$ denote the sum $\sum_i a_i$ of the p-digits of j modulo $q-1$. In this notation, the tuple for $r = \frac{q-1}{4}$ has $a_i = \frac{3p-1}{4}$ for even i and $a_i = \frac{p-3}{4}$ for odd i, while the tuple for $3r$ has the same entries but in the positions of opposite parity. We have $s(r) = s(3r) = t(p-1)$. The p-digits of $2r$ are all $\frac{p-1}{2}$, so $s(2r) = t(p-1)$ also.

By Stickelberger's Theorem [18] (see also [9, p. 636]) and the relation between Gauss sums and Jacobi sums, we know that when i, j and $i+j$ are not divisible by $q-1$ the p-adic valuation of $J(T^{-i},T^{-j})$ is equal to

$$c(i,j) := \frac{1}{p-1}(s(i)+s(j)-s(i+j)).$$

This valuation can be viewed as the number of carries, when adding the p-expansions of i and j, modulo $q-1$.

The following equations are immediate.

Lemma 4.4. *Suppose $1 \le i \le q-2$ and $i \ne r,\ 2r,\ 3r$. Then*

(i) $c(i,r) + c(q-1-i,r) = 2t$.
(ii) $c(i,r) + c(i+r,3r) + c(i+2r,r) + c(i+3r,3r) = 4t$.
(iii) $c(i,r) + c(i+2r,r) = c(i,3r) + c(i+2r,3r)$.

Theorem 4.5. (1) *The p-elementary divisors of $(\mu_L)_{|M_0}$ are $0,\ 1,\ 1,\ p^t,\ p^t$.*

(2) *For $1 \le i \le \frac{q-5}{4}$, consider the two lists $\{c(i,r), c(i+r,3r), c(i+2r,r), c(i+3r,3r)\}$ and $\{c(i,3r), c(i+r,r), c(i+2r,3r), c(i+3r,r)\}$ and let C_i be the list that contains the smallest element. Then the four p-elementary divisors of $(\mu_L)_{|M_i}$ are p^c for c in C_i.*

Proof. If X is a matrix with entries in R or a homomorphism of finitely generated, free R-modules, we let $m_j(X)$ denote the multiplicity of p^j as a p-elementary divisor and let $\kappa(X)$ denote the product of the nonzero p-elementary divisors. Thus $v_p(\kappa(X)) = \sum_j j m_j(X)$, and in the case of our Laplacian matrix, $\kappa(L) = \kappa(\mu_L)$ is the order of the p-Sylow subgroup of the critical group. We first note that for any given power p^s, if two matrices X and X' over R are equal modulo p^s then $m_j(X) = m_j(X')$ for every $j < s$. Also, we have

$$v_p(\kappa(X)) \ge \sum_{j=0}^{s-1} j m_j(X) + s(\operatorname{rank}(X) - \sum_{j=0}^{s-1} m_j(X)), \tag{4}$$

with equality if and only if the largest p-elementary divisor of X is at most p^s.

Our proof will make use of these general facts in the following way. We shall obtain a lower bound for $v_p(\kappa(L))$ by considering the matrices of $\mu_{L_{|M_i}}$ modulo q. Then we shall see that this lower bound coincides with the actual value of $v_p(\kappa(L))$ known from the Matrix-Tree Theorem, and so we must actually have equality in several inequalities used to deduce the lower bound. These inferences will enable us to complete the proof.

The matrix of $2\mu_{L_{|M_i}}$ is

$$L_i = \begin{bmatrix} q & -\alpha J(T^{-i-r}, T^{-3r}) & 0 & -\overline{\alpha} J(T^{-i-3r}, T^{-r}) \\ -\overline{\alpha} J(T^{-i}, T^{-r}) & q & -\alpha J(T^{-i-2r}, T^{-3r}) & 0 \\ 0 & -\overline{\alpha} J(T^{-i-r}, T^{-r}) & q & -\alpha J(T^{-i-3r}, T^{-3r}) \\ -\alpha J(T^{-i}, T^{-3r}) & 0 & -\overline{\alpha} J(T^{-i-2r}, T^{-r}) & q \end{bmatrix} \tag{5}$$

If we work modulo q, L_i is R-equivalent to

$$B_i = \begin{bmatrix} u_{11} J(T^{-i}, T^{-r}) & u_{12} J(T^{-i-2r}, T^{-3r}) & 0 & 0 \\ u_{21} J(T^{-i}, T^{-3r}) & u_{22} J(T^{-i-2r}, T^{-r}) & 0 & 0 \\ 0 & 0 & v_{11} J(T^{-i-3r}, T^{-3r}) & v_{12} J(T^{-i-3r}, T^{-r}) \\ 0 & 0 & v_{21} J(T^{-i-r}, T^{-r}) & v_{22} J(T^{-i-r}, T^{-3r}), \end{bmatrix} \tag{6}$$

where the u_{mn} and v_{mn} are units of R.

To apply Lemma 4.4 it is helpful to consider the matrix

$$V_i = \begin{bmatrix} c(i,r) & c(i+2r,3r) & \cdot & \cdot \\ c(i,3r) & c(i+2r,r) & \cdot & \cdot \\ \cdot & \cdot & c(i+3r,3r) & c(i+3r,r) \\ \cdot & \cdot & c(i+r,r) & c(i+r,3r) \end{bmatrix} \tag{7}$$

of the valuations of the nonzero entries of B_i.

As the entries of V_i are integers in the range $[0, 2t]$, we have equality in (4) when $X = B_i$ and $s = 2t$. Then, as B_i and L_i are R-equivalent modulo q, we have $m_j(B_i) = m_j(L_i)$

for all $j < 2t$. Thus, by applying (4) to $X = L_i$ with $s = 2t$, and noting that $\mathrm{rank}(L_i) = \mathrm{rank}(B_i) = 4$, we see that $v_p(\kappa(\mu_{L|M_i})) = v_p(\kappa(L_i)) \geq v_p(\kappa(B_i))$. By Lemma 4.4(iii), the diagonal sum of each 2×2 block of V_i is equal to the anti-diagonal sum. It follows that

(8)
$$v_p(\kappa(\mu_{L|M_i}))) = v_p(\kappa(L_i)) \geq v_p(\kappa(B_i)) \geq c(i,r)+c(i+r,3r)+c(i+2r,r)+c(i+3r,3r) = 4t.$$

where the last equality is by Lemma 4.4(ii).

The matrix of $2\mu_{L|M_0}$ is

$$\begin{bmatrix} 0 & -1 & \alpha & 0 & \overline{\alpha} \\ 0 & q & -q\alpha & 0 & -q\overline{\alpha} \\ 0 & -\overline{\alpha} & q & -\alpha J(T^{-2r}, T^{-3r}) & 0 \\ 0 & 0 & -\overline{\alpha} J(T^{-r}, T^{-r}) & q & -\alpha J(T^{-3r}, T^{-3r}) \\ 0 & -\alpha & 0 & -\overline{\alpha} J(T^{-2r}, T^{-r}) & q \end{bmatrix} \tag{9}$$

Modulo q, it is R-equivalent to

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & \alpha & 0 & \overline{\alpha} \\ 0 & -\overline{\alpha} & 0 & -\alpha J(T^{-2r}, T^{-3r}) & 0 \\ 0 & 0 & -\overline{\alpha} J(T^{-r}, T^{-r}) & 0 & -\alpha J(T^{-3r}, T^{-3r}) \\ 0 & -\alpha & 0 & -\overline{\alpha} J(T^{-2r}, T^{-r}) & 0 \end{bmatrix}. \tag{10}$$

The lower 4×4 submatrix

$$\begin{bmatrix} -1 & \alpha & 0 & \overline{\alpha} \\ -\overline{\alpha} & 0 & -\alpha J(T^{-2r}, T^{-3r}) & 0 \\ 0 & -\overline{\alpha} J(T^{-r}, T^{-r}) & 0 & -\alpha J(T^{-3r}, T^{-3r}) \\ -\alpha & 0 & -\overline{\alpha} J(T^{-2r}, T^{-r}) & 0 \end{bmatrix} \tag{11}$$

can be reduced by elementary row and column operations to

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \overline{\alpha}\alpha & \alpha J(T^{-2r}, T^{-3r}) & \overline{\alpha}^2 \\ 0 & \overline{\alpha} J(T^{-r}, T^{-r}) & 0 & \alpha J(T^{-3r}, T^{-3r}) \\ 0 & \alpha^2 & \overline{\alpha} J(T^{-2r}, T^{-r}) & \overline{\alpha}\alpha \end{bmatrix} \tag{12}$$

and the lower 3×3 block cam be further reduced to

$$\begin{bmatrix} \alpha\overline{\alpha} & \alpha J(T^{-2r}, T^{-3r}) & \overline{\alpha}^2 \\ 0 & -\alpha J(T^{-r}, T^{-r}) J(T^{-2r}, T^{-3r}) & \alpha^2 J(T^{-3r}, T^{-3r}) - \overline{\alpha}^2 J(T^{-r}, T^{-r}) \\ 0 & \overline{\alpha}^2 J(T^{-2r}, T^{-r}) - \alpha^2 J(T^{-2r}, T^{-3r}) & 0 \end{bmatrix}. \tag{13}$$

Since $c(r,r) = c(2r,3r) = c(2r,r) = c(3r,3r) = t$, we see from this last matrix form that

$$v_p(\kappa(\mu_{L|M_0})) \geq 2t. \tag{14}$$

Combining our bounds for $v_p(\kappa(\mu_{L|M_0}))$ and $v_p(\kappa(\mu_{L|M_i}))$ we see that

$$v_p(\kappa(\mu_L)) = v_p(\kappa(\mu_{L|M_0})) + \sum_{i=1}^{\frac{q-5}{4}} v_p(\kappa(\mu_{L|M_i})) \geq 2t + \frac{q-5}{4} 4t = (q-3)t = v_p(\kappa(\mu_L)), \tag{15}$$

where the last equality is from Theorem 3.2. Thus we must have equality in (14) and (8). By considering the p-adic valuation of the entries of the matrix (13), we see that equality in (14) implies immediately that its p-elementary divisors are 1, p^t and p^t, and then it follows

by considering (12) that the p-elementary divisors of $\mu_{L|M_0}$ are 0, 1, 1, p^t, p^t. This proves part (1) of the theorem.

Now we consider the consequences of all inequalities in (8) being equalities. First, we must have equality in (4) when $X = L_i$ and $s = 2t$, which shows that L_i and B_i are R-equivalent and so $\mu_{L|M_i}$ and B_i have the same p-elementary divisors. Let $B_i(1)$ and $B_i(2)$ denote the upper and lower 2×2 diagonal blocks of B_i. Equality of the second inequality in (8) implies that $v_p(\det(B_i(1)) = c(i,r) + c(i+2r,r)$ and $v_p(\det(B_i(2)) = c(i+3r,3r) + c(i+r,3r)$, since by Lemma 4.4(iii) these values were known to be lower bounds on the p-adic valuations. It is a general fact that the p-elementary divisors of any 2×2 matrix X with nonzero determinant are p^a and p^b, where a is the smallest p-adic valuation of an entry and $b = v_p(\det(X)) - a$. This shows that the p-elementary divisors of B_i are determined once the minimum valuation of an entry in each of the two blocks is known. However, we can say more, since it also follows from the definitions of $c(i)$ and the fact that $s(r) = s(3r) = t(p-1)$ that the each entry of the upper block of V_i can be obtained from corresponding entry of the lower block by adding $\frac{1}{p-1}(s(i) - s(i+r) + s(i+2r) - s(i+3r))$. Thus, the locations of the entries with lowest p-adic valuation are the same for $B_i(1)$ and $B_i(2)$. It follows that, if the lowest p-adic valuation occurs for a diagonal entry of B_i, then the p-elementary divisors of B_i are

$$p^{c(i,r)}, \quad p^{c(i+2r,r)}, \quad p^{c(i+r,3r)}, \quad p^{c(i+3r,3r)},$$

while if the lowest p-adic valuation occurs for an anti-diagonal entry of one of its blocks, then the p-elementary divisors of B_i are

$$p^{c(i+r,3r)}, \quad p^{c(i+2r,3r)}, \quad p^{c(i+r,r)}, \quad p^{c(i+3r,r)},$$

by Lemma 4.4(iii). Thus, the p-elementary divisors of B_i are determined by the smallest p-adic valuation of an entry in B_i in the manner stated in part (2) of the theorem. This concludes the proof of Theorem 4.5.

□

Corollary 4.6. *Let $m(i)$ denote the multiplicity of p^i as a p-elementary divisor of L. Then for $1 \le i \le 2t-1$ we have $m(i) = m(2t-i)$, and $m(0) = m(2t) + 2$.*

Proof. The corollary follows from Theorem 4.5 and Lemma 4.4(i). □

We can also obtain the p-rank, which was first computed in [21, Theorem 3.4].

Corollary 4.7. $\operatorname{rank}_p L = 2(3^t - 1)(\frac{p+1}{4})^{2t}$

Proof. We know that the p-rank of $\mu_{L|M_0}$ is 2, so we need to count the occurrences of 1 as a p-elementary divisor in the $\mu_{L|M_i}$ for $1 \le i \le \frac{q-5}{4}$.

We note that if we swap the rows and columns of the lower block of the matrix C in (7) (which corresponds to swapping the same rows and columns in (6)) we obtain a block sum of two matrices, both of the form

$$\begin{bmatrix} c(j,r) & c(j+2r,3r) \\ c(j,3r) & c(j+2r,r) \end{bmatrix} \tag{16}$$

for suitable j, and that as j runs from 1 to $\frac{q-5}{4}$, the entries in the blocks form the multiset

$$\{c(\ell,r), c(\ell,3r) \mid 1 \le \ell \le q-1, \ell \ne 0, r, 2r, 3r\}$$

By examining just the 0-th p-digit, it is easy to see that if $c(j,r) = 0$, then $c(j+2r,r) > 0$. Likewise, if $c(j,3r) = 0$, then $c(j+2r,3r) > 0$. This means that (16) has at most one zero on the diagonal and at most one zero on the anti-diagonal. In view of Lemma 4.4(iii), there

can be at most one p-elementary divisor equal to 1 in the corresponding block (6), and this will occur if and only if there is at least one zero entry in (16). With these observations in hand, it is now a simple matter to count the number of blocks with a nonzero entry by counting the sets $\{i \mid c(i,r) = 0\}$, $\{i \mid c(i,3r) = 0\}$, $\{i \mid c(i,r) = 0 \text{ and } c(i,3r) = 0\}$, and $\{i \mid c(i,r) = 0 \text{ and } c(i+2r,3r) = 0\}$. The first set consists of those i whose even index p-digits are $\leq \frac{3p-1}{4}$ and whose odd index p-digits are $\leq \frac{p-3}{4}$, so this set has size $(\frac{3(p+1)}{4})^t(\frac{(p+1)}{4})^t$. Similarly, the second set has the same size, while the last two sets have size $(\frac{(p+1)}{4})^{2t}$. The result follows. □

The following examples give an idea of the size and structure of the critical groups.

Our first example, which is small enough for hand computation using Theorem 4.5, provides an alternative proof to the one in [16] that $P^*(9^2)$ and Paley(9^2) are not isomorphic.

Example 4.8. Let $q = 9^2$. We shall write a 3-digit expression $a_0 + a_1 3 + a_2 3^2 + a_3 3^3$ as a tuple (a_0, a_1, a_2, a_3). Then $r = 20 = (2, 0, 2, 0)$ and $3r = 60 = (0, 2, 0, 2)$. We must find the lists C_i for $1 \leq i \leq \frac{q-5}{4} = 19$. First we compute the list $\{i, i+r, i+2r, i+3r\}$ and then by inspection one can see whether adding r or $3r$ to something in this list will produce the fewest carries. If, for example the fewest carries are produced by adding $3r$ to $i+2r$, then we alternately add r or $3r$ to every entry of the list, in the unique way such that $3r$ is added to $i+2r$. Then C_i is the list recording the number of carries in these operations. For example, when $i = 6$, we compute the list $\{6, 26, 46, 66\} = \{(0,2,0,0), (2,2,2,0), (1,0,2,1), (0,1,1,2)\}$. It is obvious that adding $(2,0,2,0)$ to $(0,2,0,0)$ produces zero carries, so we perform the following additions: $(0,2,0,0) + (2,0,2,0)$ (0 carries); $(2,2,2,0) + (0,2,0,2)$ (4 carries); $(1,0,2,1) + (2,0,2,0)$ (2 carries); $(0,1,1,2) + (0,2,0,2)$ (2 carries). Thus, $C_6 = \{0,4,2,2\}$. In this way, we find the sets C_i in Theorem 4.5, and obtain

$$K(P^*(9^2)) \cong (\mathbb{Z}/20\mathbb{Z})^{40} \oplus [(\mathbb{Z}/3Z)^{20} \oplus (\mathbb{Z}/9\mathbb{Z})^{10} \oplus (\mathbb{Z}/27\mathbb{Z})^{20} \oplus (\mathbb{Z}/81\mathbb{Z})^{14}].$$

The critical group of the Paley graphs are given in [5].

$$K(\text{Paley}(9^2)) \cong (\mathbb{Z}/20\mathbb{Z})^{40} \oplus [(\mathbb{Z}/3Z)^{16} \oplus (\mathbb{Z}/9\mathbb{Z})^{18} \oplus (\mathbb{Z}/27\mathbb{Z})^{16} \oplus (\mathbb{Z}/81\mathbb{Z})^{14}].$$

By implementing Theorem 4.5 on a computer algebra system such as *sage* we can compute the critical groups of larger examples than would be possible by working directly with the Laplacian matrix.

Example 4.9. The critical group $K(P^*(3^{12}))$ is isomorphic to

$$\begin{aligned}(\mathbb{Z}/132860\mathbb{Z})^{265720} \oplus [&(\mathbb{Z}/3\mathbb{Z})^{11376} \oplus (\mathbb{Z}/3^2\mathbb{Z})^{33408} \oplus (\mathbb{Z}/3^3\mathbb{Z})^{54176} \oplus (\mathbb{Z}/3^4\mathbb{Z})^{66852} \\ &\oplus (\mathbb{Z}/3^5\mathbb{Z})^{66420} \oplus (\mathbb{Z}/3^6\mathbb{Z})^{64066} \oplus (\mathbb{Z}/3^7\mathbb{Z})^{66420} \oplus (\mathbb{Z}/3^8\mathbb{Z})^{66852} \\ &\oplus (\mathbb{Z}/3^9\mathbb{Z})^{54176} \oplus (\mathbb{Z}/3^{10}\mathbb{Z})^{33408} \oplus (\mathbb{Z}/3^{11}\mathbb{Z})^{11376} \oplus (\mathbb{Z}/3^{12}\mathbb{Z})^{1454}].\end{aligned}$$

5. Paley and Peisert graphs with over fields of order p^2, with $p \equiv 3 \pmod 4$.

Assume that $q = p^{2t}$, $p \equiv 3 \pmod 4$. In this section we shall use $A(q)$ to denote the adjacency matrix of Paley(q) and $A^*(q)$ to denote the adjacency matrix of $P^*(q)$, both with respect to some arbitrary but fixed ordering on their common vertex set $\mathbb{F}_q$. The graphs Paley(q) and $P^*(q)$ are cospectral, but in the special case when $q = p^2$, we shall show that they are even more closely related.

Let D be an integral domain and let D_n denote the ring of $n \times n$ matrices with entries in D. We shall say that two matrices A and B in D_n are *similar over* D if, and only if, there is

an invertible element C of D_n such that $CAC^{-1} = B$. If P is a prime ideal of D, we denote be D_P the localization of D at P.

Theorem 5.1. *Assume $q = p^2$ with $p \equiv 3 \pmod 4$.*

(i) *$A(q)$ and $A^*(q)$ are similar over the ring of algebraic integers in some number field.*
(ii) *$A(q)$ and $A^*(q)$ are similar over $\mathbb{Z}_{(\ell)}$, the ring of ℓ-local integers, for every prime $\ell \in \mathbb{Z}$.*

Before giving the proof of Theorem 5.1 we discuss its implications. Since the Smith normal form of a matrix is determined locally, that is, one prime at a time, any two matrices that satisfy the equivalent conditions of Theorem 5.1 have the same Smith normal form.

By Theorem 5.1, it is immediate that for any a, $b \in \mathbb{Z}$ the matrices $aA(q) + bI$ and $aA^*(q) + bI$ are cospectral and have the same Smith normal form. Since Paley(q) and $P^*(q)$ are strongly regular graphs with the same parameters $(k, \lambda, \mu) = (\frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$, the equation

$$A^2 + (\mu - \lambda)A + (\mu - k)I = \mu J, \tag{17}$$

satisfied by both $A(q)$ and $A^*(q)$, implies that any matrix C with $CA(q)C^{-1} = A^*(q)$ must commute with J and therefore transforms the generalized adjacency matrix $aA(q) + bI + cJ$ to $aA^*(q) + bI + cJ$ for any a, b and c. We arrive at the following corollary.

Corollary 5.2. *Let $q = p^2$, $p \equiv 3 \pmod 4$. For any integers a, b and c, the generalized adjacency matrices $aA(q) + bI + cJ$ and $aA^*(q) + bI + cJ$ are cospectral and have the same Smith normal forms.* □

We now turn to the proof of Theorem 5.1. We shall make use of the following "local-global" theorem of Guralnick [10, Theorem 7], based on results of Reiner-Zassenhaus [17], Taussky [19] and Dade [6].

Theorem 5.3. *Let D be the ring of integers of a finite extension of $\mathbb{Q}$. Suppose A, $B \in D_n$. Then the following are equivalent.*

(i) *A and B are similar over D_P for each prime ideal P of D.*
(ii) *A and B are similar over some finite integral extension of D.*

□

Lemma 5.4. *Assume $q = p^{2t}$ with $p \equiv 3 \pmod 4$. Let $\ell \neq p$ be a prime and let Λ be a prime ideal lying over ℓ in the cyclotomic ring $\mathbb{Z}[\zeta]$, where ζ is a primitive p-th root of unity in an algebraic closure of $\mathbb{Q}$. Then $A(q)$ and $A^*(q)$ are similar over the localization $\mathbb{Z}[\zeta]_\Lambda$.*

Proof. Let X be the character table of $(\mathbb{F}_q, +)$, considered as a matrix with entries in $\mathbb{Z}[\zeta]$. By the orthogonality relations X is invertible over the ring $\mathbb{Z}[\zeta][\frac{1}{p}]$. It has long been known (cf. [14]) that the adjacency matrix of an abelian Cayley graph can be transformed to diagonal form using the character table, so

$$XA(q)X^{-1} = E, \qquad \text{and} \qquad XA^*(q)X^{-1} = E^*, \tag{18}$$

where E and E^* are the diagonal matrices of eigenvalues in some order. Since $A(q)$ and $A^*(q)$ are cospectral, there is a permutation matrix P such that $PEP^{-1} = E^*$. Therefore, we have

$$(X^{-1}PX)A(q)(X^{-1}PX)^{-1} = A^*(q). \tag{19}$$

We may regard this as an equation in the ring of matrices over $\mathbb{Z}[\zeta][\frac{1}{p}]$, and since for every $\ell \neq p$ and any prime ideal Λ of $\mathbb{Z}[\zeta]$ containing ℓ, we have $\mathbb{Z}[\zeta][\frac{1}{p}] \subseteq \mathbb{Z}[\zeta]_\Lambda$, the lemma is proved. □

In order to complete the proof of Theorem 5.1 it suffices to show that $A(p^2)$ and $A^*(p^2)$ are similar over the ring R of §4. For then we may apply Theorem 5.3 first with D being the ring of integers in $\mathbb{Q}(\zeta, \xi)$ to deduce (i), and a second time with with $D = \mathbb{Z}$ to deduce (ii). We assume p to be fixed from now on. As similarity of $A(p^2)$ and $A^*(p^2)$ is equivalent to similarity of $K = 2A(p^2) + I$ and $K^* = 2A^*(p^2) + I$, we shall consider the latter matrices, as they have a more convenient form.

By [5, Lemma 3.1], the matrix of μ_K on M_i with respect to the ordered basis e_i, e_{i+2r}, e_{i+r}, e_{i+3r} is

$$K_i = \begin{bmatrix} 0 & J(i+2r,2r) & 0 & 0 \\ J(i,2r) & 0 & 0 & 0 \\ 0 & 0 & 0 & J(i+3r,2r) \\ 0 & 0 & J(i+r,2r) & 0 \end{bmatrix} \tag{20}$$

The matrix of μ_{K^*} on M_i with respect to the ordered basis e_i, e_{i+2r}, e_{i+r}, e_{i+3r} is

$$K_i^* = \begin{bmatrix} 0 & 0 & \alpha J(i+r,3r) & \overline{\alpha} J(i+3r,r) \\ 0 & 0 & \overline{\alpha} J(i+r,r) & \alpha J(i+3r,3r) \\ \overline{\alpha} J(i,r) & \alpha J(i+2r,3r) & 0 & 0 \\ \alpha J(i,3r) & \overline{\alpha} J(i+2r,r) & 0 & 0 \end{bmatrix} \tag{21}$$

The matrix of μ_K on M_0 with respect to the ordered basis $\mathbf{1}$, $[0]$, e_{2r}, e_r, e_{3r} is

$$K_0 = \begin{bmatrix} q & 1 & -1 & 0 & 0 \\ 0 & 0 & q & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & J(3r,2r) \\ 0 & 0 & 0 & J(r,2r) & 0 \end{bmatrix} \tag{22}$$

The matrix μ_{K^*} on M_0 with respect to the ordered basis $\mathbf{1}$, $[0]$, e_r, e_{2r}, e_{3r} is

$$K_0^* = \begin{bmatrix} q & 1 & -\alpha & 0 & -\overline{\alpha} \\ 0 & 0 & q\alpha & 0 & q\overline{\alpha} \\ 0 & \overline{\alpha} & 0 & \alpha J(2r,3r) & 0 \\ 0 & 0 & \overline{\alpha} J(r,r) & 0 & \alpha J(3r,3r) \\ 0 & \alpha & 0 & \overline{\alpha} J(2r,r) & 0 \end{bmatrix} \tag{23}$$

Our aim is to show that K_i and K_i^* are similar over R. We first dispose of the similarity of K_0 and K_0^*.

We shall need some results on Gauss and Jacobi sums over the field of p^2 elements, which follow immediately from [2, Theorem 2.12] and the well known formula expressing a Jacobi sum of two characters as the product of their Gauss sums divided by the Gauss sum of their product character.

Lemma 5.5.
(i) $J(r,r) = J(3r,3r) = J(r,2r) = J(3r,2r) = p$.
(ii) *For* $1 \leq i \leq q-2$ *and* $i \notin \{r, 2r, 3r\}$ *we have* $J(i,r)J(i+r,r) = J(i,3r)J(i+3r,3r)$. □

Let $v_1 = \mathbf{1}$, $v_2 = [0]$, $v_3 = \overline{\alpha}e_r + \alpha e_{3r}$, $v_4 = e_{2r}$, $v_5 = \alpha e_r + \overline{\alpha}e_{3r}$. Using the relations $\alpha^2 = -\frac{\eta}{2}$, $\overline{\alpha}^2 = \frac{\eta}{2}$ and $\alpha\overline{\alpha} = \frac{1}{2}$, and Lemma 5.5 it is easy to check that indeed the v_i form a basis of M_0 and that the matrix of μ_{K^*} on M_0 in this new basis is the matrix K_0. We have thus established the similarity of K_0 and K_0^*.

Lemma 5.6. (i) *For $1 \le i \le \frac{q-1}{4}$ the eigenvalues of each 2×2 block of K_i are p and $-p$.*

(ii) *For $1 \le i \le q-2$ and $i \notin \{r, 2r, 3r\}$ we have $J(i, 2r)J(i + 2r, 2r) = p^2$.*

(iii) *The eigenvalues of K_i^* are p and $-p$, each with multiplicity 2.*

Proof. The eigenvalues of K and K^* on $R^{\mathbb{F}_q}$ are p^2, with multiplicity 1 and eigenvector $\mathbf{1}$, and p and $-p$, with equal multiplicity. It follows that on any invariant subspace not containing $\mathbf{1}$ on which K (respectively K^*) has trace 0, the eigenvalues are p and $-p$ with equal multiplicity, so (i) and (iii) hold. Then (ii) follows from (i) and (20). □

Lemma 5.7. *Let $1 \le i \le \frac{q-1}{4}$. Then K_i is similar to the matrix in the following list which has the same p-rank as K_i.*

$$\begin{bmatrix} 0 & p & 0 & 0 \\ p & 0 & 0 & 0 \\ 0 & 0 & 0 & p \\ 0 & 0 & p & 0 \end{bmatrix}, \begin{bmatrix} 0 & p^2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & p \\ 0 & 0 & p & 0 \end{bmatrix}, \begin{bmatrix} 0 & p^2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & p^2 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{24}$$

Proof. We choose a new basis $v_1 = e_i$, $v_2 = p^{-c(i,2r)}J(i, 2r)e_{i+2r}$, $v_3 = e_{i+r}$, $v_4 = p^{-c(i+r,2r)}J(i+r, 2r)e_{i+3r}$. Then, by Lemma 5.6(ii), the matrix of μ_K on M_i is the matrix in (24) that has the same p-rank as K_i. □

For $1 \le i \le \frac{q-1}{4}$, let $J(i) = \{i, i + r, i + 2r, i + 3r\}$ Then for $j \in J(i)$, the vectors e_j, e_{j+r}, e_{j+2r}, e_{j+r} are just the vectors e_i, e_{i+r}, e_{i+2r}, e_{i+2r} in a different order, so the matrix, which we shall call K_j^* of μ_{K^*} on M_i with respect to the first ordered basis is similar to K_i^* (by a permutation matrix). This gives us the flexibility to talk about K_j^* for any j with $1 \le j \le q-2$, $j \notin \{r, 2r, 3r\}$. We will show for each i with $1 \le i \le \frac{q-1}{4}$, that K_j^* is similar over R to K_i for some $j \in J(i)$.

We consider the matrix of p-adic valuations of the entries in K_i^*:

$$\begin{bmatrix} 0 & 0 & c(i + r, 3r) & c(i + 3r, r) \\ 0 & 0 & c(i + r, r) & c(i + 3r, 3r) \\ c(i, r) & c(i + 2r, 3r) & 0 & 0 \\ c(i, 3r) & c(i + 2r, r) & 0 & 0 \end{bmatrix}. \tag{25}$$

From the definition of $c(i, j)$ and the fact that $s(r) = s(3r) = (p - 1)$ can be written in the form

$$\begin{bmatrix} 0 & 0 & d + D & b + D \\ 0 & 0 & c + D & a + D \\ a & b & 0 & 0 \\ c & d & 0 & 0 \end{bmatrix}, \tag{26}$$

where $D = \frac{1}{p-1}(s(i) - s(i + r) + s(i + 2r) - s(i + 3r))$ and the entries a, b, c, d, $a + D$, $b + D$, $c + D$, $d + D$ lie in the set $\{0, 1, 2\}$.

Lemma 5.8. (i) $a + d = b + c$.

(ii) $a + d + b + c + 2D = 4$, *so* $a + d + D = 2$.

(iii) $D \in \{-1, 0, 1\}$. *Hence* $a + d > 0$.

Proof. Parts (i) and (ii) are special cases of parts (ii) and (iii) of Lemma 4.4. By (ii) we know $|D| \leq 2$. If $D = 2$, then by (ii), we must have $a = b = c = d = 0$. If $D = -2$, then by (ii), we must have $a = b = c = d = 2$ and the upper right matrix is zero. So, by replacing i by $i + r$ if necessary, we can assume that $D = 2$ and that $a = b = c = d = 0$, in order to reach a contradiction. Now $a = c(i, r)$ and $c = c(i, 3r)$. Let $i = (i_0, i_1)$ and recall that $r = (\frac{3p-1}{4}, \frac{p-3}{4})$ and $r = (\frac{p-3}{4}, \frac{3p-1}{4})$. In order for $a = c = 0$, we must have $0 \leq i_0, i_1 \leq \frac{p-3}{4}$. But then if $i + 2r = (j_0, j_1)$, we have $\frac{p-1}{2} \leq j_0, j_1$, which forces $c(i + 2r, r) > 0$, contrary to the assumption that $d = 0$. The final assertion is clear. □

Lemma 5.9. *K_i^* and K_i have the same p-rank, for $1 \leq i \leq \frac{q-1}{4}$.*

Proof. We have already seen that the $\mathrm{rank}_p(K_i) \in \{0, 1, 2\}$. To see that $\mathrm{rank}_p(K_i^*) \in \{0, 1, 2\}$, we simply note that each of the anti-diagonal 2×2 blocks in K_i^* must be singular modulo p, by Lemma 5.8(iii). We will prove that $\mathrm{rank}_p(K_i^*) = 2$ if $\mathrm{rank}_p(K_i) = 2$ and $\mathrm{rank}_p(K_i^*) = 0$ if $\mathrm{rank}_p(K_i) = 0$. Suppose $\mathrm{rank}_p(K_i) = 2$. Then, by replacing i by some $j \in J(i)$ if necessry, we can assume that $c(i, 2r) = 0 = c(i + r, 2r)$. We shall show that $c(i, 3r) = 0$ and $c(i + r, r) = 0$. Since these entries occur in different anti-diagonal 2×2 blocks, this will force $\mathrm{rank}_p(K_i^*) = 2$. Let $i = (i_0, i_1)$ and $i + r = (j_0, j_1)$. The hypotheses mean that i_0, i_1, j_0, $j_1 \leq \frac{p-1}{2}$. Since $\frac{3p-1}{4} \geq \frac{p-1}{2} \geq j_0$, when $r = (\frac{3p-1}{4}, \frac{p-3}{4})$ is added to i a carry must be generated by the addition of the first digits. This implies that $i_0 > \frac{p-3}{4}$. Since $\frac{p-3}{4} + 1 + \frac{p-1}{2} \leq p - 1$, no carry is generated from the addition of the second digits of r and i. Thus, $j_1 = i_1 + \frac{p-3}{4} + 1$. Since $j_1 \leq \frac{p-1}{2}$, we deduce that $i_1 \leq \frac{p+1}{4} - 1 = \frac{p-3}{4}$. It is then easily checked that $c(i, 3r) = 0$. Also, since $j_0 + p = i_0 + \frac{3p-1}{4}$, we have $j_0 \leq \frac{p-3}{4}$, from which it follows that $c(i + r, r) = 0$. We have proved that $\mathrm{rank}_p(K_i^*) = 2$ if $\mathrm{rank}_p(K_i) = 2$. Next suppose that $\mathrm{rank}_p(K_i) = 0$. Since $\det(K_i) = p^4$, we must have $c(i, 2r) = c(i + r, 2r) = c(i + 2r, 2r) = c(i + 3r, 2r) = 1$. Since $s(2r) = p - 1$, we deduce from the formula $c(u, v) = \frac{1}{p-1}(s(u) + s(v) - s(u + v))$ that $s(i) = s(i+r) = s(i+2r) = s(i+3r)$. It then follows that all of the nonzero entries of (25) are equal to 1, so that $\mathrm{rank}_p(K_i^*) = 0$. □

We are now ready to complete the proof of similarity of K_i and K_i^*. We have seen that $\mathrm{rank}_p(K_i^*) = \mathrm{rank}_p(K_i) \in \{0, 1, 2\}$. For each p-rank, we exhibit a basis of M_i for which the matrix of the restriction of μ_{K^*} is the corresponding matrix in (24).

Suppose $\mathrm{rank}_p(K_i^*) = 0$. Then all nonzero entries of (21) are exactly divisible by p. We set $v_1 = e_i$ $v_2 = \frac{1}{p}(\overline{\alpha}J(i, r)e_{i+r} + \alpha J(i, 3r)e_{i+3r})$, $v_3 = e_{i+2r}$, and $v_4 = \frac{1}{p}(\alpha J(i+2r, 3r)e_{i+r} + \overline{\alpha}J(i + 2r, r)e_{i+3r})$. It is easy to check that v_1, v_2, v_3 and v_4 form a basis of M_i. Then $\mu_{K^*}(v_1) = pv_2$ and

$$
\begin{aligned}
\mu_{K^*}(v_2) &= \frac{1}{p}[\overline{\alpha}J(i, r)\mu_{K^*}(e_{i+r}) + \alpha J(i, 3r)\mu_{K^*}(e_{i+3r})] \\
&= \frac{1}{p}[\overline{\alpha}J(i, r)(\alpha J(i + r, 3r)e_i + \overline{\alpha}J(i + r, r)e_{i+2r}) \\
&\quad + \alpha J(i, 3r)(\overline{\alpha}J(i + 3r, r)e_i + \alpha J(i + 3r, 3r)e_{i+2r})] \qquad (27) \\
&= \frac{1}{p}\overline{\alpha}\alpha[J(i, r)J(i + r, 3r) + J(i, 3r)J(i + 3r, r))]e_i \\
&\quad + \frac{1}{p}[\overline{\alpha}^2 J(i, r)J(i + r, r) + \alpha^2 J(i, 3r)J(i + 3r, 3r)]e_{i+2r}
\end{aligned}
$$

By Lemma 5.5(ii), and the fact that $\alpha^2 + \overline{\alpha}^2 = 0$, we see that the coefficient of e_{i+2r} is zero. Thus v_1 and v_2 span a μ_{K^*}-invariant subspace on which μ_{K^*} has trace zero, hence determinant $-p^2$. It follows that the coefficient of v_1 must be p. The same calculation with i replaced by $i + 2r$ shows that $\mu_{K^*}(v_3) = pv_4$ and $\mu_{K^*}(v_4) = pv_3$, so with respect to the basis v_1, v_2, v_3, v_4, the matrix of μ_{K^*} on M_i is the first matrix in (24).

Suppose $\mathrm{rank}_p(K_i^*) = 1$. Then, $D \neq 0$ as otherwise the p-rank would be even. Up to replacing i by some $j \in J(i)$, we can assume $D = 1$. Then by a further change of i with $i + 2r$ if necessary we can assume that the matrix (25) of valuations is

$$\begin{bmatrix} 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \tag{28}$$

We set $v_1 = e_i$ $v_2 = \overline{\alpha}J(i,r)e_{i+r} + \alpha J(i,3r)e_{i+3r}$, $v_3 = e_{i+2r}$, and $v_4 = \frac{1}{p}(\alpha J(i+2r,3r)e_{i+r} + \overline{\alpha}J(i+2r,r)e_{i+3r})$. It is straightforward to check that v_1, v_2, v_3 and v_4 form a basis for M_i and a similar calculation to the p-rank 0 case shows that on M_i the matrix of μ_{K^*} with respect to this basis is the second matrix of (24).

Suppose $\mathrm{rank}_p(K_i^*) = 2$. Then, we must have $D = 0$, since neither anti-diagonal block can have p-rank 0. Up to replacing i by $j \in J(i)$, we can assume that in (25) $c(i,3r) = c(i+3r,r) = 0$, whence $c(i+2r,3r) = c(i+r,r) = 2$, by Lemma 5.8(ii). We claim that $c(i,r) = c(i+2r,r) = 1$. Suppose not. Then one of $c(i,r)$ and $c(i+2r,r)$ is zero and the other is 2. If $c(i,r) = 0$ and $c(i+2r,r) = 2$, let $i = (i_0, i_1)$. Since also $c(i,3r) = 0$, we must have i_0, $i_1 \leq \frac{p-3}{4}$. Then $i + 2r = (i_0 + \frac{p-1}{2}, i_1 + \frac{p-1}{2})$, with $i_1 + \frac{p-1}{2} \leq \frac{3p-5}{4} = \frac{3p-1}{4} - 1$. This means that in adding r to $i + 2r$, there can be no carry generated in the second digit, which contradicts the assumption that $c(i+2r,r) = 2$. If $c(i,r) = 2$ and $c(i+2r,r) = 0$, we obtain a contradiction similarly. Thus, we may assume that the matrix of valuations (25) is

$$\begin{bmatrix} 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \tag{29}$$

We set $v_i = e_i$ $v_2 = \overline{\alpha}J(i,r)e_{i+r} + \alpha J(i,3r)e_{i+3r}$, $v_3 = e_{i+2r}$, and $v_4 = \alpha J(i+2r,3r)e_{i+r} + \overline{\alpha}J(i+2r,r)e_{i+3r}$, and easily check that these vectors form a basis of M_i. Then a similar calculation to the p-rank 0 case, shows that the matrix of μ_{K^*} with respect to this basis is the third matrix of (24).

The proof that K_i and K_i^* are similar over R is now complete.

Remark 5.10. For $p > 3$ we do not know when, if ever, $A(p^2)$ and $A^*(p^2)$ are similar over $\mathbb{Z}$.

References

[1] Hua Bai, *On the critical group of the n-cube*, Linear Algebra Appl. **369** (2003), 251–261.

[2] Bruce C. Berndt and Ronald J. Evans, *Sums of gauss, eisenstein, jacobi, jacobsthal, and brewer*, Illinois J. Math. **23** (1979), no. 3, 374–437.

[3] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1998, A Wiley-Interscience Publication. MR 1625181 (99d:11092)

[4] A. E. Brouwer and W. H. Haemers, *Spectra of graphs*, Universitext, Springer, New York, 2012. MR 2882891

[5] David B. Chandler, Peter Sin, and Qing Xiang, *The Smith and critical groups of Paley graphs*, J. Algebraic Combin. **41** (2015), no. 4, 1013–1022.
[6] E. C. Dade, *Algebraic integral representations by arbitrary forms*, Mathematika **10** (1963), 96–100.
[7] D. Dhar, *Self-organized critical state of sandpile automaton models*, Phys. Rev. Lett. **64** (1990), no. 14, 1613–1616.
[8] Joshua E. Ducey and Deelan M. Jalil, *Integer invariants of abelian Cayley graphs*, Linear Algebra Appl. **445** (2014), 316–325.
[9] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648. MR 0140494 (25 #3914)
[10] Robert M. Guralnick, *A note on the local-global principle for similarity of matrices*, Linear Algebra Appl. **30** (1980), 241–245.
[11] B. Jacobson, Critical groups of graphs, Honors Thesis, University of Minnesota, 2003; http://www.math.umn.edu/reiner/HonorsTheses/Jacobson thesis.pdf.
[12] Brian Jacobson, Andrew Niedermaier, and Victor Reiner, *Critical groups for complete multipartite graphs and Cartesian products of complete graphs*, J. Graph Theory **44** (2003), no. 3, 231–250.
[13] D. Lorenzini, *Smith normal form and Laplacians*, J. Combin. Theory Ser. B **98** (2008), no. 6, 1271–1300. MR 2462319 (2010d:05092)
[14] F. J. MacWilliams and H. B. Mann, *On the p-rank of the design matrix of a difference set*, Information and Control **12** (1968), 474–488. MR 0242696 (39 #4026)
[15] Natalie Mullin, *Self-complementary arc-transitive graphs and their imposters*, Master thesis, U. Waterloo (2009).
[16] Wojciech Peisert, *All self-complementary symmetric graphs*, J. Algebra **240** (2001), no. 1, 209–229. MR 1830551 (2002e:05074)
[17] I. Reiner and H. Zassenhaus, *Equivalence of representations under extensions of local ground rings.*, Illinois J. Math. **5** (1961), 409–411.
[18] L. Stickelberger, *Ueber eine Verallgemeinerung der Kreistheilung*, Math. Ann. **37** (1890), no. 3, 321–367. MR 1510649
[19] Olga Taussky, *A Diophantine problem arising out of similarity classes of integral matrices*, J. Number Theory **11** (1979), no. 3 S. Chowla Anniversary Issue, 472–475.
[20] A. Vince, *Elementary divisors of graphs and matroids*, European J. Combin. **12** (1991), no. 5, 445–453.
[21] Guobiao Weng, Weisheng Qiu, Zeying Wang, and Qing Xiang, *Pseudo-Paley graphs and skew Hadamard difference sets from presemifields*, Des. Codes Cryptogr. **44** (2007), no. 1-3, 49–62. MR 2336393 (2008g:05031)
[22] Melanie Matchett Wood, *The distribution of sandpile groups of random graphs.* arxiv math.PR/1402.5149v2 (2015).

Department of Mathematics, University of Florida, P. O. Box 118105, Gainesville FL 32611, USA