DIFFERENCE FAMILIES, SKEW HADAMARD MATRICES, AND CRITICAL GROUPS OF DOUBLY REGULAR TOURNAMENTS.

VENKATA RAGHU TEJ PANTANGI

Abstract. In this paper we investigate the structure of the critical groups of doubly regular tournaments (DRTs) associated with skew Hadamard difference families (SDFs) with one, two, or four blocks. In [20], the existence of a skew Hadamard matrix of order $n+1$ was found to be equivalent to the existence of a DRT on n vertices. A well known construction of a skew Hadamard matrix order n is by constructing skew Hadamard difference sets in abelian groups of order $n-1$. The Paley skew Hadamard matrix is an example of one such construction. Szekeres [25, 26] and Whiteman [29] constructed skew Hadamard matrices from skew Hadamard difference families with two blocks. Wallis and Whiteman [28] constructed skew Hadamard matrices from skew Hadamard difference families with four blocks. In this paper we consider the critical groups of DRTs associated with skew Hadamard matrices constructed from skew Hadamard difference families with one, two or four blocks. We compute the critical groups of DRTs associated with skew Hadamard difference families with two or four blocks. We also compute the critical group of the Paley tournament and show that this tournament is inequivalent to the other DRTs we considered. Consequently we prove that the associated skew Hadamard matrices are not equivalent.

1. Introduction.

A Hadamard matrix H of order n is an $n\times n$ matrix of $+1$'s and -1's such that $HH^{\intercal} = nI$. It is well known that if n is the order of a Hadamard matrix, then $n = 1, 2$ or $n \equiv 0 \pmod 4$. It is conjectured that Hadamard matrices of order n exist for all $n \equiv 0 \pmod 4$. The smallest n for which there is no known Hadamard matrix is $n = 668$ (c.f. [11]). In this paper we deal with skew Hadamard matrices. A Hadamard matrix H is said to be skew if $H + H^{\intercal} = 2I$.

Two Hadamard matrices are considered equivalent if one can be obtained from the other by negating rows or columns, or by interchanging rows or columns. It is of interest to determine the equivalence of Hadamard matrices of the same order. Every Hadamard matrix of order n is equivalent to a Hadamard matrix of the form $\begin{bmatrix} 1 & \mathbf{1}_{n-1}^{\intercal} \\ -\mathbf{1}_{n-1} & H_0 \end{bmatrix}$. All the Hadamard matrices we consider in this paper are assumed to be in this form.

In this paper, we are interested in the inequivalence of skew Hadamard matrices. If H_1 and H_2 are two Hadamard matrices of same order but with different Smith normal forms, then they are inequivalent. In [14], it was found that the Smith normal form of any skew Hadamard matrix of order $4m$ is $\mathrm{diag}[1, \underbrace{2, \ldots, 2}_{2m-1}, \underbrace{2m, \ldots, 2m}_{2m-1}, 4m]$. So Smith normal form fails to distinguish inequvivalent skew Hadamard matrices of the same order. In this article we consider a different invariant associated with skew Hadamard matrices.

A tournament T_n of order n is a directed graph obtained by assigning directions to every edge of a complete graph on n vertices. Given vertices v, w of T_n, by $d(v)$ we denote the outdegree of v and by $d(v, w)$ we denote the number of vertices dominated by v and w. A DRT with parameters (n, k, λ) is a tournament of order n such that for every pair of distinct vertices $v,\ w$, we have $d(v) = k$ and $d(v, w) = \lambda$. It is easy to see that $n = 4\lambda + 3$ and $k = 2\lambda + 1$. Theorem 2 of [20] shows that a skew Hadamard matrix of order $n + 1$ exists if and only if there is a DRT on n vertices. Given a Hadamard H matrix of order $4\lambda + 4$, the matrix M which is obtained by deleting the first column and row of $\frac{1}{2}(J - H)$ is the adjacency matrix of a DRT with parameters $(4\lambda + 3, 2\lambda + 1, \lambda)$. Here J is the matrix of all ones. Now if $\tilde{M}$ is the adjacency matrix of a DRT with parameters $(4\lambda + 3, 2\lambda + 1, \lambda)$, then $\tilde{H} = \begin{bmatrix} 1 & \mathbf{1}_{4\lambda+3}^{\intercal} \\ -\mathbf{1}_{4\lambda+3} & J-2\tilde{M} \end{bmatrix}$ is a skew Hadamard matrix. Any invariant of the DRT graph associated with a skew Hadamard matrix H is an equivalence preserving invariant of H. In this paper, we look at the critical groups of DRTs.

Let $\Gamma = (V, E)$ be a finite, connected, loopless, possibly directed graph on vertex set V with edge set $E \subset V \times V$. We say that a vertex v dominates a vertex w if $(v, w) \in E$. By Δ_v we denote the number of vertices dominated by v. By $\mathbb{Z}^V$ we denote the free abelian group with V as a basis set. Then the adjacency map $\nu_M : \mathbb{Z}^V \to \mathbb{Z}^V$ that maps $v \in V$ to the

Key words and phrases. invariant factors, elementary divisors, Smith normal form, critical group, sandpile group, Laplacian, doublyregular tournament, skew Hadamard matrix, skew Hadamard difference family.

formal sum of vertices dominated by v, encodes adjacency of the graph. The map $\nu_Q : \mathbb{Z}^V \to \mathbb{Z}^V$ that maps $v \in V$ to $\Delta_v v - \nu_M(v)$ is called the Laplacian map. The *critical* group $\mathcal{K}$ of Γ is the finite part of the cokernal of ν_Q. The critical group is an invariant of the graph. Now let β be an ordered basis of $\mathbb{Z}^V$ that is obtained by fixing an order on V. The adjacency matrix M of Γ is the matrix representation of ν_M with respect to β. We define the Laplacian matrix Q to be the matrix representation of ν_Q with respect to β. Let Δ be the diagonal matrix whose vth diagonal entry is Δ_v. Then we have $Q = \Delta - M$. If Q_v is the matrix obtained by deleting the vth row and vth column of Q, then the Matrix-tree theorem (eg. [22, 5.64 and 5.68]) states that $|det(Q_v)|$ is the number of oriented trees in Γ with root v. If Γ is a directed Eulerian graph, $det(Q_v)$ is independent of the vertex v and $|\mathcal{K}| = |det(Q_v)|$. If Γ is undirected, $|\mathcal{K}| = |det(Q_v)|$ is the number of spanning trees of Γ. For a nice survey on critical groups of graphs, we refer to [23, §3]. Some papers with computations of critical groups of families of graphs include [27], [13], [12], [5], [2], [10], [8], [4], [19], and [18]. In [12], Lorenzini examined the proportion of graphs with cyclic critical groups among graphs with critical groups of particular order.

One effective way of constructing skew Hadamard matrices/DRTs is by using skew difference families. Let $(G, +)$ be an additive finite abelian group of order n. A *skew difference family* (SDF) on l blocks with parameters (n, k, λ) is a family $\{B_i | 1 \le i \le l\}$ of k-subsets such that for all $1 \le i \le l$ and $g \in G \setminus \{0_G\}$, we have (i) $|\{(x, y) \in \bigcup_{i=1}^{l} B_i \times B_i \mid g = x - y\}| = \lambda - 1$, (ii) $B_i \cap -B_i = \emptyset$, and (iii) $B_i \cup -B_i = G \setminus \{0_G\}$. An SDF with one block in G is called a skew Hadamard difference set.

We will now describe a few SDFs found in literature. The earliest construction is that of the Paley difference set by Paley [17]. It was conjectured that Paley difference set was the only(upto equvivalence) SDF with one block. Ding and Yuan [7] disproved the conjecture by constructing other SDFs with one block. Szekeres [25, 26], Whiteman [29] found an SDF with two blocks in $(\mathbb{F}_q, +)$, where either $q \equiv 5 \pmod 8$; or $q = p^e$ with $p \equiv 5 \pmod 8$ a prime and $e \equiv 2 \pmod 4$. Wallis and Whiteman [28] constructed an SDF with four blocks in $(\mathbb{F}_q, +)$, where $q \equiv 9 \pmod{16}$. Momihara and Xiang [15] generalised the constructions by Szekres, Wallis and Whiteman to obtain the following result.

Proposition 1. [15, Theorem 1.5] *Let $u \ge 2$ be an integer and q be a prime power such that $q \equiv 2^u + 1 \pmod{2^{u+1}}$. Then for any positive integer e, there exists a skew Hadamard difference family with 2^{u-1} blocks in $(\mathbb{F}_{q^e}, +)$.*

Szekeres [25] also proved the following result.

Proposition 2. [25, Theorem 3] *Let q be a prime power such that $q \equiv 3 \pmod 4$. Then, there exists a skew Hadamard difference family with 2 blocks in $(\mathbb{Z}/n\mathbb{Z}, +)$, where $n = \frac{q-1}{2}$.*

In this paper, we compute the critical groups of the three families of DRTs described below. Given $X \subset G$, by δ_X we denote the characteristic function of X in G.

(i) Let $(G, +)$ be an additive abelian group of order $2\lambda + 1$ and (A, B) be an SDF with two blocks in G, with parameters $(2\lambda + 1, \lambda, \lambda - 1)$. Then $\mathcal{SZ}(G, A, B)$ is the graph with vertex set $V = \{v_0\} \cup \{a_g | \, g \in G\} \cup \{b_g | \, g \in G\}$, whose adjacency map $\nu_M : \mathbb{Z}^V \to \mathbb{Z}^V$ satisfies

$$\begin{aligned} \nu_M(v_0) &= \sum_{x \in G} a_x \\ \nu_M(a_g) &= \sum_{z \in G} \delta_A(z) a_{g+z} + \sum_{z \in G} \delta_{B \cup \{0_G\}}(z) b_{g+z} \\ \nu_M(b_g) &= v_0 + \sum_{z \in G} \delta_{-A}(z) b_{g+z} + \sum_{z \in G} \delta_{B \cup \{0_G\}}(z) a_{g+z} \end{aligned} \quad , \tag{1}$$

for all $g \in G$. Theorem 2 of [25] shows that $\mathcal{SZ}(G, A, B)$ is a DRT with parameters $(4\lambda + 3, 2\lambda + 1, \lambda)$. Setting $u = 2$ in Proposition 1 provides us with a famiy of SDFs with two blocks. Proposition 2 provides another such family. Theorem 4 describes the critical group of $\mathcal{SZ}(G, A, B)$. We utilize the natural action of group G on the vertex set of $\mathcal{SZ}(G, A, B)$ to compute the Smith normal form of its Laplacian.

(ii)Let $(G, +)$ be an additive abelian group of order $2\lambda + 1$ and (A, B, C, D) be an SDF with four blocks in G, with parameters $(2\lambda + 1, \lambda, \lambda - 1)$.

Then by $\mathcal{W}(G, A, B, C, D)$ we denote a graph with vertex set $V = \{v_1, v_2, v_3\} \bigcup_{\mu=a,b,c,d} V_\mu$. Here $V_\mu = \{\mu_g |\ g \in G\}$. We require the adjacency map $\mu_M : \mathbb{Z}^V \to \mathbb{Z}^V$ of $\mathcal{W}(G, A, B, C, D)$ to satisfy

$$\begin{aligned}
\nu_M(v_1) &= \sum_{x\in G} a_x + \sum_{x\in G} c_x \\
\nu_M(v_2) &= \sum_{x\in G} a_x + \sum_{x\in G} d_x \\
\nu_M(v_3) &= \sum_{x\in G} a_x + \sum_{x\in G} b_x \\
\nu_M(a_g) &= \sum_{z\in G} \delta_A(z) a_{g+z} + \sum_{z\in G} \delta_{B\cup\{0_G\}}(z) b_{g+z} + \sum_{z\in G} \delta_{-C\cup\{0_G\}}(z) c_{z-g} + \sum_{z\in G} \delta_{D\cup\{0_G\}}(z) d_{(z+g)} \qquad , \\
\nu_M(b_g) &= v_1 + v_2 + \sum_{z\in G} \delta_B(z) a_{g+z} + \sum_{z\in G} \delta_{-A}(z) b_{g+z} + \sum_{z\in G} \delta_{-D}(z) c_{(g+z)} + \sum_{z\in G} \delta_{C\cup\{0_G\}}(z) d_{z-g} \\
\nu_M(c_g) &= v_2 + v_3 + \sum_{z\in G} \delta_C(z) a_{z-g} + \sum_{z\in G} \delta_{-D\cup\{0_G\}}(z) b_{g+z} + \sum_{z\in G} \delta_A(z) c_{(g+z)} + \sum_{z\in G} \delta_B(z) d_{(g+z)} \\
\nu_M(d_g) &= v_1 + v_3 + \sum_{z\in G} \delta_D(z) a_{g+z} + \sum_{z\in G} \delta_C(z) b_{z-g} + \sum_{z\in G} \delta_{B\cup\{0_G\}}(z) c_{(g+z)} + \sum_{z\in G} \delta_{-A}(z) d_{(g+z)}
\end{aligned} \tag{2}$$

for all $g \in G$.

Let $(g_1, g_2, \ldots, g_{2\lambda+1})$ be an ordering on G. Consider the ordered basis

$$\beta = (v_1, v_2, v_3, a_{g_1}, \ldots, a_{g_{2\lambda+1}},\ b_{g_1}, \ldots, b_{g_{2\lambda+1}},\ c_{g_1}, \ldots, c_{g_{2\lambda+1}},\ d_{g_1}, \ldots, d_{g_{2\lambda+1}}).$$

Let M be the matrix representation of μ_M with respect to β.

Theorem 12 of [28] states that $\begin{bmatrix} 1 & \mathbf{1}^\intercal_{8\lambda+3} \\ -\mathbf{1}_{8\lambda+3} & J-2M \end{bmatrix}$ is a skew Hadamard matrix. Using this we see that $\mathcal{W}(G, A, B, C, D)$ is a DRT with parameters $(8\lambda + 7, 4\lambda + 3, 2\lambda + 1)$. Setting $u = 3$ in Proposition 1 provides us with a famiy of SDFs with four blocks. Theorem 5 describes the critical group of $\mathcal{W}(G, A, B, C, D)$. We utilize the natural action of group G on the vertex set of $\mathcal{W}(G, A, B, C, D)$ to compute the Smith normal form of its Laplacian.

(iii) The third family we consider is the family of Paley tournaments. Let A be a skew Hadamard difference set in an abelian group G of order $4\lambda + 3$. By $DRT(G, A)$ we denote the graph with vertex set $\{[g]|\ g \in G\}$ and arc set $\{([g], [h])|\ h - g \in A\}$. The adjacency map $\nu_M : \mathbb{Z}^G \to \mathbb{Z}^G$ satisfies $\nu_M([g]) = \sum_{z\in G} \delta_A(z)[g + z]$. Let p^t be a power of a prime p with $q \equiv 3 \pmod 4$ and let $\mathbb{F}_q$ be the finite field of order q. Let H be the set of non-zero squares in $\mathbb{F}_q$. It is well known that H is a skew Hadamard difference set in the additive group $(\mathbb{F}_q, +)$ of the field. The Paley tournament graph $\mathcal{P}(q)$ is $DRT(G, H)$, that is, it is the Cayley graph on $(\mathbb{F}_q, +)$ with "connection" set being the multiplicative subgroup of squares in $\mathbb{F}_q$. Theorem 7 describes the critical group of $\mathcal{P}(q)$. This was essentially computed in [5], in which the authors describe the critical group of the Paley graph. This computation involves some Jacobi sums involving the quadratic character ψ. The only difference between our computation here and that in [5] is that $\psi(-1) = -1$ in our case.

2. Main results.

Let $\mathcal{K}$ be the critical group of a DRT with parameters $(4\lambda + 3, 2\lambda + 1, \lambda)$, by $\mathcal{K}_1$ we denote the subgroup of order $(\lambda + 1)^{2\lambda+1}$. Let $\mathcal{K}_2$ be the subgroup of $\mathcal{K}$ of order $(4\lambda + 3)^{2\lambda}$. We observe that $\mathcal{K} = \mathcal{K}_1 \oplus \mathcal{K}_2$. In §4 we show that $\mathcal{K}_1$ depends only on the parameter λ.

Theorem 3. *Let λ be a positive integer and let $\mathcal{K}$ denote the critical group of a DRT with parameters $(4\lambda+3, 2\lambda+1, \lambda)$. Then $\mathcal{K} = (\mathbb{Z}/(\lambda + 1)\mathbb{Z})^{2\lambda+1} \oplus \mathcal{K}_2$, where $\mathcal{K}_2$ is a subgroup of order $(4\lambda + 3)^{2\lambda}$.*

The result below describes the critical group of $\mathcal{SZ}(G, A, B)$. We prove this in §5.

Theorem 4. *Let λ be a positive integer and let (A, B) be an SDF in an additive abelian G with $|G| = 2\lambda + 1$. Let Q denote the Laplacian matrix of $\mathcal{SZ}(G, A, B)$ and by $\mathcal{K}$ we denote its critical group. Then $\mathcal{K} = (\mathbb{Z}/(\lambda + 1)\mathbb{Z})^{2\lambda+1} \oplus (\mathbb{Z}/(4\lambda + 3)\mathbb{Z})^{2\lambda}$. Let $\mathfrak{p}$ be a prime and let $\mathrm{rk}_\mathfrak{p}(Q)$ denote the $\mathfrak{p}$-rank of Q. If $\mathfrak{p} \mid \lambda + 1$, then $\mathrm{rk}_\mathfrak{p}(Q) = 2\lambda + 1$; and if $\mathfrak{p} \mid 4\lambda + 3$, then $\mathrm{rk}_\mathfrak{p}(Q) = 2\lambda + 2$.*

The result below describes the critical group of $\mathcal{W}(G, A, B, C, D)$. We prove this in §6.

Theorem 5. *Let λ be a positive integer and let (A, B, C, D) be an SDF in an additive abelian G with $|G| = 2\lambda+1$. Let Q denote the Laplacian matrix of $\mathcal{W}(G, A, B, C, D)$ and by $\mathcal{K}$ we denote its critical group. Then $\mathcal{K} = (\mathbb{Z}/(2\lambda+2)\mathbb{Z})^{4\lambda+3} \oplus (\mathbb{Z}/(8\lambda+7)\mathbb{Z})^{4\lambda+2}$. Let $\mathfrak{p}$ be a prime and let $\mathrm{rk}_{\mathfrak{p}}(Q)$ denote the $\mathfrak{p}$-rank of Q. If $\mathfrak{p} \mid \lambda+1$, then $\mathrm{rk}_{\mathfrak{p}}(Q) = 4\lambda+3$; and if $\mathfrak{p} \mid 4\lambda+3$, then $\mathrm{rk}_{\mathfrak{p}}(Q) = 4\lambda+4$.*

The following describes the critical group of $\mathcal{P}(q)$. We prove this in §7.

Theorem 6. *Let p be a prime and t be a positive integer such that $q := p^t \equiv 3 \pmod 4$. Let Q denote the Laplacian matrix of $\mathcal{P}(q)$ and by $\mathcal{K}$ we denote its critical group. Then the p-rank of Q is $\left(\frac{p+1}{2}\right)^t$ and $\mathcal{K} = (\mathbb{Z}/\mu\mathbb{Z})^{2\mu} \bigoplus_{i=1}^{t} \left(\mathbb{Z}/p^i\mathbb{Z}\right)^{e_i}$, where*

(1) $\mu = \frac{q-1}{4}$;

(2) $e_t = \left(\frac{p+1}{2}\right)^t - 2$;

(3) and for $1 \le i < t$,

$$e_i = \sum_{j=0}^{\min\{i,t-i\}} \frac{t}{t-j}\binom{t-j}{j}\binom{t-2j}{i-j}(-p)^j\left(\frac{p+1}{2}\right)^{t-2j}.$$

Remark 1. Let q be a prime power satisfying $q \equiv 3 \pmod 4$. Proposition 2 provides us with an SDF with two blocks in $G := \mathbb{Z}/n\mathbb{Z}$, where $n = \frac{q-1}{2}$. Let (A, B) be an SDF in G. Both $\mathcal{P}(q)$ and $\mathcal{SZ}(G, A, B)$ are DRT's with parameters $(q, (q-1)/2, (q-3)/4)$. Theorems 4 and 6 show that these graphs have non isomorphic critical groups. Therefore these graphs are not isomorphic and thus the associated Hadamard matrices are not equivalent.

Remark 2. Let $\tilde{q}$ be a prime power such that $\tilde{q} \equiv 5 \pmod 8$. Proposition 1 guarantees the existence of an SDF with two blocks in $(\mathbb{F}_q, +)$. Let (A, B) be an SDF in $(\mathbb{F}_{\tilde{q}}, +)$. Let's also assume that $q = 2\tilde{q}+1$ is also a power of a prime. Theorems 4 and 6 show that that $\mathcal{SZ}(\mathbb{F}_{\tilde{q}}, A, B)$ and $\mathcal{P}(q)$ are not isomorphic and thus the associated Hadamard matrices are not equivalent.

Remark 3. Let $\tilde{q}$ be a prime power such that $\tilde{q} \equiv 9 \pmod{16}$. Proposition 1 guarantees the existence of an SDF with four blocks in $(\mathbb{F}_q, +)$. Let (A, B, C, D) be an SDF in $(\mathbb{F}_{\tilde{q}}, +)$. Let's also assume that $q = 4\tilde{q}+3$ is also a power of a prime. Theorems 5 and 6 show that that $\mathcal{W}(\mathbb{F}_{\tilde{q}}, A, B, C, D)$ and $\mathcal{P}(q)$ are not isomorphic and thus the associated Hadamard matrices are not equivalent.

Remark 4. We found that the critical groups of $\mathcal{SZ}(G, A, B)$ and $\mathcal{W}(G, A, B, C, D)$ depend only on the order of G. However this is not the case for DRTs constructed from skew Hadamard difference sets. Let $q \equiv 3 \pmod 4$ be a prime power. To construct $\mathcal{P}(q)$, the set H of quadratic residues in $(\mathbb{F}_q, +)$ was used. Another example of skew Hadamard difference set is the set $DY(1) = \{x^{10} - x^6 - x^2 | \ x \in \mathbb{F}_{3^n}^{\times}\}$ in the additive group $(\mathbb{F}_{3^n}, +)$, with n odd. This was constructed by Ding and Yuan [7]. By $DRT(3^n, DY(1))$, we denote the DRT with vertex set $\{[x] | \ x \in \mathbb{F}_{3^n}\}$ and arc set $\{([x], [y]) | \ y - x \in DY(1)\}$. With the help of a computer, we can find that the SNFs of the Laplacians of $DRT(3^5, DY(1))$ and $\mathcal{P}(243)$ are different. It was conjectured in [6] that there are at least five inequvivalent difference sets in $(\mathbb{F}_{3^n}, +)$ for all odd $n > 3$.

3. Preliminaries

3.1. **Smith Normal Forms.** Let $\mathfrak{R}$ be a Principal Ideal Domain and $Z : \mathfrak{R}^m \to \mathfrak{R}^n$ be a linear transformation. By the structure theorem for finitely generated modules over PIDs, we have $\{s_i(Z)\}_{i=1}^{r} \subset \mathfrak{R} \setminus \{0\}$ such that $s_i(Z) \mid s_{i+1}(Z)$ and

$$\mathrm{coker}(Z) \cong \mathfrak{R}^{n-r} \oplus \bigoplus_{i=1}^{r} \mathfrak{R}/s_i(Z)\mathfrak{R}.$$

Let $[Z]$ denote the matrix representation of Z with respect to the standard bases. Then the above equation tells us that we can find $P \in \mathrm{GL}_n(\mathfrak{R})$, and $Q \in \mathrm{GL}_m(\mathfrak{R})$ such that

$$P[Z]Q = \left[\begin{array}{c|c} Y & 0_{(r\times n-r)} \\ \hline 0_{(m-r\times r)} & 0_{(n-r\times n-r)} \end{array}\right],$$

where $Y = \mathrm{diag}(s_1(Z), \ldots, \ s_r(Z))$. The diagonal form $P[Z]Q$ is called the Smith normal form (SNF) of Z. Its uniqueness (up to multiplication of $s_i(Z)$'s by units) is also guaranteed by the aforementioned structure theorem. By invariant factors (elementary divisors) of Z, we mean the invariant factors (respectively elementary divisors) of the module coker(Z). In this section, we collect some useful results about Smith normal forms.

The following is a well known result (for eg. see Theorem 2.4 of [23]) that gives a description of the Smith normal form in terms of minor determinants.

Lemma 7. *Let Z, $[Z]$, and $\{s_i(Z)\}_{1\leq i\leq r}$ be as described above. Given $1 \leq i \leq r$, let $d_i(Z)$ be the GCD of all $i \times i$ minor determinants of $[Z]$, and let $d_0(Z) = 1$. We then have $s_i(Z) = d_i([Z])/d_{i-1}([Z])$.*

The following result which is Theorem 1 of [16] gives a relation between SNF of the product of two matrices and the SNFs of the individual matrices.

Lemma 8. *Let $\Re$ be a principal ideal domain. Given $M \in M_n(\Re)$ and $1 \leq k \leq n$, by $s_k(M)$ we denote the kth invariant factor of M. If $A,\ B \in M_n(\Re)$, then for $1 \leq k \leq n$ we have $s_k(A) \mid s_k(AB)$ and $s_k(B) \mid s_k(AB)$.*

Consider a prime $\mathfrak{p} \in \Re$ and a square matrix N with entries in $\Re$, whose SNF over $\Re$ is
$\operatorname{diag}(s_1(N), \dots, s_iN, \dots s_n(N))$.

Let $\mathcal{S}_\mathfrak{p}$ be any unramified extension of the local ring $\Re_\mathfrak{p}$. If $\operatorname{diag}(\mathfrak{p}^{j_1}, \dots, \mathfrak{p}^{j_i}, \dots, p^{j_n})$ is the SNF of N considered as a matrix over $\mathcal{S}_\mathfrak{p}$, then $\mathfrak{p}^{j_i} \| s_i(N)$. So while finding Smith normal forms, we can focus on one prime at a time.

3.2. **Properties of DRTs.** Let λ be a positive integer. By M be we denote the adjacency matrix of a DRT with parameters $(4\lambda+3, 2\lambda+1, \lambda)$, then $Q := (2\lambda+1)I - M$ is its Laplacian matrix. Using the definition of DRTs, we can easily deduce that $M + M^\intercal = J - I$ and $MM^\intercal = (\lambda+1)I + \lambda J$. Thus we have

$$Q + Q^\intercal = (4\lambda+3)I - J \tag{3}$$

and

$$QQ^\intercal = (4\lambda+3)(\lambda+1)I - (\lambda+1)J. \tag{4}$$

The following is a well know result about adjacency matrices of DRTs.

Lemma 9. *Let λ be a positive integer and let Γ be a DRT with parameters $(4\lambda+3, 2\lambda+1, \lambda)$. Let M and Q be the adjaceny matrix and Laplacian matrix respectively, of Γ. By $\mathcal{K}$ we denote the critical group of Γ. Then*

i $(x-k)(x^2+x+\lambda+1)^{2\lambda+1}$ *is the characteristic polynomial of M;*

ii the eigenvalues of Q are 0, $\dfrac{4\lambda+3-\left(\sqrt{4\lambda+3}\right)i}{2}$, and $\dfrac{4\lambda+3+\left(\sqrt{4\lambda+3}\right)i}{2}$, with multiplicities 1, k, and k respectively;

iii and $|\mathcal{K}| = (4\lambda+3)^{2\lambda}(\lambda+1)^{2\lambda+1}$.

Proof. Using $Q = (2\lambda+1)I - M$, we see that (i) implies (ii). Matrix tree theorem shows that (ii) implies (iii).

Using $M+M^\intercal = J-I$ and $MM^\intercal = (\lambda+1)I+\lambda J$, we have $\det(xI-M)\det(xI-M^\intercal) = \det((x-\lambda)J+(x^2+x+\lambda+1)I)$. Observing that $\det(aI+bJ) = (a+(4\lambda+3)b)a^{4\lambda+2}$ and that $\det(xI-M) = \det(xI-M^\intercal)$, we arrive at (i). □

3.3. **Permutation action and characters.** We will now collect some useful results from character theory. Each of $\mathcal{P}(q)$, $\mathcal{SZ}(G, A, B)$, $\mathcal{W}(G, A, B, C, D)$ is constructed using a finite abelian group $(G, +)$. We use the natural action of G on the vertex set to compute the critical groups. These actions are closely related to the regular action of G on itself.

We define the action of G on $Y = \{y_g \mid g \in G\}$ by $h.y_g = y_{g+h}$. This is the regular action of G. Let $\mathfrak{p} \nmid |G|$ be a prime and let $\mathfrak{S}$ be an extension of $\mathbb{Q}_\mathfrak{p}$ containing the $|G|$-th roots of unity. By R we denote the ring of integers of $\mathfrak{S}$, and by R^Y we denote the free R-module generated by Y as a basis set. Let $Irr(G)$ be the group of R-valued characters of G.

It is well known from representation theory that the RG-permutation module R^Y decomposes into direct sum of non-isomorphic RG-modules of R-rank 1, affording characters $\chi \in Irr(G)$. A basis element for the module affording χ is $e_{(y,\chi)} = \sum_{g\in G}\chi(-g)y_g$. The following Lemma is useful in our computations.

Lemma 10. *Let $X \subset G$, and let $\delta_X : G \to R$ be the characteristic function of X in G. Let $\chi(X) := \sum_{z\in X}\chi(z)$. Then we have*

(1) $\sum_{g\in G}\chi(-g)\sum_{z\in G}\delta_X(z)y_{g+z} = \chi(X)e_{(y,\chi)}$ *and*

(2) $\sum_{g\in G}\chi(-g)\sum_{z\in G}\delta_X(z)y_{z-g} = \overline{\chi(X)}e_{(y,\chi^{-1})}$.

Proof. Using $\chi(-g) = \chi(-z)\chi(z-g) = \chi^{-1}(z)\chi^{-1}(g-z)$, we see that

$$\sum_{z\in G}\chi^{-1}(z)\delta_X(z)\sum_{g\in G}\chi^{-1}(g-z)y_{z-g} = (\chi^{-1}(X))e_{(y,\chi^{-1})}.$$

We may conclude (2) by using $\overline{\chi(X)} = \chi^{-1}(X)$. Proof of (1) follows via similar rearrangements. □

4. Description of $\mathcal{K}_1$.

In this section we prove Theorem 3. Let Q be the Laplacian matrix of a DRT with parameters $(4\lambda+3, 2\lambda+1, \lambda)$. Let $\mathcal{K}$ denote its critical group, then from Lemma 9, we have $|\mathcal{K}| = (4\lambda+3)^{2\lambda}(\lambda+1)^{2\lambda+1}$. As $4\lambda+3$ and $\lambda+1$ are coprime,there are subgroups $\mathcal{K}_1, \mathcal{K}_2$ of $\mathcal{K}$ such that $|\mathcal{K}_1| = (\lambda+1)^{2\lambda+1}$, $|\mathcal{K}_2| = (4\lambda+3)^{2\lambda}$, and $\mathcal{K} = \mathcal{K}_1 \oplus \mathcal{K}_2$. Theorem 3 describes the structure of $\mathcal{K}_1$ for all DRTs.

We extend the arguments used in [14] to determine the structure of $\mathcal{K}_1$. Let $\mathfrak{p} \mid \lambda+1$ be a prime integer. Then the Smith normal form of Q over the $\mathfrak{p}$-adic numbers $\mathbb{Z}_\mathfrak{p}$ gives us the $\mathfrak{p}$-part of $\mathcal{K}_1$. Let $s_1(Q), \dots, s_{4\lambda+3}(Q)$ be the invariant factors of Q considered as a matrix over $\mathbb{Z}_\mathfrak{p}$

From (4) we see that $QQ^\intercal \equiv 0 \pmod{\mathfrak{p}}$. Therefore we have $\mathrm{rk}_\mathfrak{p}(Q) \le 4\lambda+3-\mathrm{rk}_\mathfrak{p}(Q^\intercal)$ and thus $\mathrm{rk}_\mathfrak{p}(Q) \le 2\lambda+1$. Using (3), we see that $Q + Q^\intercal \equiv -I - J \pmod{\mathfrak{p}}$. So,

$$\begin{aligned} 4\lambda+2 &= \mathrm{rk}_\mathfrak{p}(I+J) \\ &= \mathrm{rk}_\mathfrak{p}(Q+Q^\intercal) \\ &\le 2\mathrm{rk}_\mathfrak{p}(Q), \end{aligned}$$

and thus $\mathrm{rk}_\mathfrak{p}(Q) = 2\lambda+1$. So $s_i(Q)$ is a unit in $\mathbb{Z}_p$ for $1 \le i \le 2\lambda+1$.

Using $SNF((4\lambda+3)(\lambda+1)I - (\lambda+1)J) = \mathrm{diag}(\lambda+1,\ (4\lambda+3)(\lambda+1), \dots,\ (4\lambda+3)(\lambda+1),\ 0)$, equation (4), and Lemma 8 we may conclude that (i) $s_1(Q) \mid s_1(QQ^\intercal) = 4\lambda+3$; (ii) $s_{4\lambda+3}(Q) \mid s_{4\lambda+3}(QQ^\intercal) = 0$; (iii) and $s_i(Q) \mid (4\lambda+3)(\lambda+1)$ for $1 < i < 4\lambda+3$. We recall that $v_\mathfrak{p}\left(\prod_{i=1}^{4\lambda+2} s_i(Q)\right) = v_\mathfrak{p}\left((4\lambda+3)^{2\lambda}(\lambda+1)^{2\lambda+1}\right)$. Since for $1 \le i \le 2\lambda+1$, $s_i(Q)$ is a unit in $\mathbb{Z}_p$, we have $\left(\prod_{i=2\lambda+2}^{4\lambda+2} s_i(Q)\right) = v_\mathfrak{p}\left((4\lambda+3)^{2\lambda}(\lambda+1)^{2\lambda+1}\right)$. As $s_i(Q) \mid \lambda+1$, we can now conclude that $s_i(Q) = \lambda+1$ for $2\lambda+2 \le i \le 4\lambda+2$. It now follows that $\mathcal{K}_1 = (\mathbb{Z}/(\lambda+1)\mathbb{Z})^{2\lambda+1}$.

5. Crtical group of $\mathcal{SZ}(G, A, B)$.

Let us turn our attention to DRTs of the form $\mathcal{SZ}(G,A,B)$. Let (A,B) be an SDF in an abelian group $(G,+)$ of order $2\lambda+1$. By $\mathcal{SZ}(G,A,B)$ we denote the graph with vertex set $V = \{v_0\} \cup \{a_g | \, g \in G\} \cup \{b_g | \, g \in G\}$ and whose adjacency operator ν_M satisfies (1).

We recall that $\mathcal{SZ}(G,A,B)$ is a DRT with parameters $(4\lambda+3, 2\lambda+1, \lambda)$. Let Q be the Laplacian matrix of $\mathcal{SZ}(G,A,B)$ and $\mathcal{K}$ be its critical group. By Theorem 3, we have $\mathcal{K} = (\mathbb{Z}/(\lambda+1)\mathbb{Z})^{2\lambda+1} \oplus \mathcal{K}_2$, where $\mathcal{K}_2$ is the subgroup of order $(4\lambda+3)^{2\lambda}$. Let $\mathfrak{p} \mid 4\lambda+3$ be a prime. Determining the SNF of Q over an unramified extension of $\mathbb{Z}_\mathfrak{p}$ will give us the $\mathfrak{p}$-part of $\mathcal{K}_2$.

Let $t \in \mathbb{N}$ such that $|G| \mid (\mathfrak{p}^t - 1)$, by θ we denote a primitive $(\mathfrak{p}^t-1)$st root of unity in $\mathbb{Q}_\mathfrak{p}$. We denote by $\mathcal{R}$, the ring of integers in $\mathbb{Q}(\theta)$. As $\mathfrak{p}$ is unramified in $\mathcal{R}$, the $\mathfrak{p}$-part of $\mathcal{K}$ can be found by determining the SNF of Q over $\mathcal{R}$. By $\mathcal{R}^V$, we denote the free module over $\mathcal{R}$ with V as a basis set. The matrix Q defines a map $\nu_Q : \mathcal{R}^V \to \mathcal{R}^V$ with $\nu_Q(x) = (2\lambda+1)x - \nu_M(x)$.

We now consider the action of $(G,+)$ on V that satisfies (i)$h.v_0 = v_0$, (ii) $h.a_g = a_{g+h}$, and (iii)$h.b_g = b_{g+h}$ for all $g, h \in G$. This permutation action preserves adjacency. The action of G on V makes $\mathcal{R}^V$ a permutation module for G. Given $\chi \in Irr(G)$, we define $N_\chi := \{x \in \mathcal{R}^V | g.x = \chi(g)x \text{ for all } g \in G\}$. In other words, N_χ is the direct sum of all irreducible submodules of $\mathcal{R}^V$ affording χ. As G preserves adjacency, ν_Q is an $\mathcal{R}G$ map. Now by applying Schur's Lemma, we have $\nu(N_\chi) \subset N_\chi$.

The action of G decomposes $\mathcal{R}^V$ into $\mathcal{R}^{\{v_0\}} \oplus \mathcal{R}^{V_a} \oplus \mathcal{R}^{V_b}$, where $V_\mu = \{\mu_g | g \in G\}$ for $\mu = a, b$. Now $\mathcal{R}^{V_\mu}$ is a regular module for G, and $\mathcal{R}^{\{v_0\}}$ is a trivial module. Now $\mathcal{R}^{V_\mu} = \bigoplus_{\chi\in Irr(G)} M_{(\chi,\mu)}$, where $M_{(\chi,\mu)}$ is the submodule affording χ. A basis element for $M_{(\chi,\mu)}$ is $e_{(\mu,\chi)} = \sum_{g\in G}\chi(-g)\mu_g$.

Let χ_0 denote the trivial character of G. For $\chi \neq \chi_0$, we have $N_\chi = M_{(\chi,a)} + M_{(\chi,b)}$; and $N_{\chi_0} = Rv + M_{(\chi_0,a)} + M_{(\chi_0,b)}$. We now have $R^V = \bigoplus_{\chi\in Irr(G)} N_\chi$, with $\nu_Q(N_\chi) \subset N_\chi$. We will now look at $\nu_Q|_{N_\chi}$.

Using Lemma 10 and the relations in (1) yields the following lemma.

Lemma 11. *Let $\chi \in Irr(G) \setminus \{\chi_0\}$, then*

(1) $\nu_Q(e_{(\chi,a)}) = (2\lambda + 1 - \chi(A))e_{(\chi,a)} + (-1 - \chi(B))e_{(\chi,b)}$ *and*

(2) $\nu_Q(e_{(\chi,b)}) = (-\chi(B))e_{(\chi,a)} + (2\lambda + 1 - \chi(-A))e_{(\chi,b)}$.

For $\chi \neq \chi_0$, let Q_χ be the matrix representation of $\nu_Q|_{N_\chi}$ with respect to the ordered basis $(e_{(\chi,a)}, e_{(\chi,b)})$. let Q_{χ_0} be the matrix representation of $\nu_Q|_{N_{\chi_0}}$ with respect to the ordered basis $(e_{(\chi_0,a)}, e_{(\chi_0,b)}, v)$. So Q is similar to the block diagonal matrix $\bigoplus_{\chi\in Irr(G)} Q_\chi$.

We see from Lemma 11 that for $\chi \neq \chi_0$, we have $Tr(Q_\chi) = 4\lambda + 2 - \chi(A) - \chi(-A)$. Now as χ is not trivial, we have $0 = \chi(G)$. Using $A \cup -A = G \setminus \{0_G\}$, we may conclude that $Tr(Q_\chi) = 4\lambda + 3$. The eigenvalues of Q_χ are elements of the set $\left\{0, \frac{4\lambda+3-\left(\sqrt{4\lambda+3}\right)i}{2}, \frac{4\lambda+3+\left(\sqrt{4\lambda+3}\right)i}{2}\right\}$ of eigenvalues of Q. As $Tr(Q_\chi) = 4\lambda + 3$, the eigenvalues of Q_χ are $\frac{4\lambda+3-\left(\sqrt{4\lambda+3}\right)i}{2}$ and $\frac{4\lambda+3+\left(\sqrt{4\lambda+3}\right)i}{2}$ and $det(Q_\chi) = (4\lambda + 3)(\lambda + 1)$.

We also observe from Lemma 11 that the difference of the off-diagonal entries of Q_χ is 1 and thus one of them is coprime to $\mathfrak{p}$. Applying Lemma 7 and $det(Q_\chi) = (4\lambda+3)(\lambda+1)$ we can conclude that $\mathrm{diag}(1, 4\lambda+3)$ is the SNF of Q_χ over $\mathcal{R}$. Similar computations can be used to show that $\mathrm{diag}(1, 1, 0)$ is the SNF of Q_{χ_0} over $\mathcal{R}$. This proves Theorem 4.

6. Crtical group of $\mathcal{W}(G, A, B, C, D)$.

Given an SDF (A, B, C, D) in an additive abelian group $(G, +)$ of order $2\lambda + 1$, we recall that $\mathcal{W}(G, A, B, C, D)$ is a graph with vertex set $V = \{v_1, v_2, v_3\} \bigcup_{\mu=a,b,c,d} \{\mu_g | \, g \in G\}$, and whose adjacency operator ν_M is defined by (2).

We recall that $\mathcal{W}(G, A, B, C, D)$ is a DRT with parameters $(8\lambda + 7, 4\lambda + 3, 2\lambda + 2)$. Let Q be the Laplacian matrix of $\mathcal{W}(G, A, B, C, D)$ and $\mathcal{K}$ be its critical group. By Theorem 3, we have $\mathcal{K} = (\mathbb{Z}/(2\lambda + 2)\mathbb{Z})^{4\lambda+3} \oplus \mathcal{K}_2$, where $\mathcal{K}_2$ is the subgroup of order $(8\lambda + 7)^{4\lambda+2}$. Let $\mathfrak{p} \mid 8\lambda + 7$ be a prime Determining the SNF of Q over an unramified extension of $\mathbb{Z}_\mathfrak{p}$ will give us the $\mathfrak{p}$-part of $\mathcal{K}_2$.

Let $t \in \mathbb{N}$ such that $|G| \mid (\mathfrak{p}^t - 1)$, by θ we denote a primitive $(\mathfrak{p}^t - 1)$st root of unity in $\mathbb{Q}_\mathfrak{p}$. We denote by $\mathcal{R}$, the ring of integers in $\mathbb{Q}(\theta)$. As $\mathfrak{p}$ is unramified in $\mathcal{R}$, the $\mathfrak{p}$-part of $\mathcal{K}$ can be found by determining the SNF of Q over $\mathcal{R}$. By $\mathcal{R}^V$, we denote the free module over $\mathcal{R}$ with V as a basis set. The matrix Q defines a map $\nu_Q : \mathcal{R}^V \to \mathcal{R}^V$ with $\nu_Q(x) = (4\lambda + 3)x - \nu_M(x)$.

Unlike in the case of $\mathcal{SZ}(G, A, B)$, the natural G action on $\mathcal{W}(G, A, B, C, D)$ does not preserve adjacency, but provides a useful integral basis for $\mathcal{R}^V$. We consider the action of G on V that satisfies (i)$h.v_i = v_i$, (ii) $h.\mu_g = \mu_{g+h}$ for all $(i, g, h, \mu) \in \{1, 2, 3\} \times G \times G \times \{a, b, c, d\}$.

The action of G decomposes $\mathcal{R}^V$ into $\bigoplus_{i=1}^{3} \mathcal{R}^{\{v_i\}} \oplus \bigoplus_{\mu=a,b,c,d} \mathcal{R}^{V_\mu}$, where $V_\mu = \{\mu_g | g \in G\}$. Now $\mathcal{R}^{V_\mu}$ is a regular module of G, and $\mathcal{R}^{\{v_i\}}$'s are trivial modules. Now $\mathcal{R}^{V_\mu} = \bigoplus_{\chi\in Irr(G)} M_{(\chi,\mu)}$, where $M_{(\chi,\mu)}$ is the submodule affording χ. A basis element for $M_{(\chi,\mu)}$ is $e_{(\mu,\chi)} = \sum_{g\in G} \chi(-g)\mu_g$. The following Lemma describes the images of $e_{(\mu,\chi)}$ under the action of ν_Q.

Lemma 12. *For non-trivial $\chi \in Irr(G)$, we have*

(1) $\nu_Q(e_{(a,\chi)}) = (4\lambda + 3 - \chi(A))e_{(a,\chi)} + (\overline{\chi(B)})e_{(b,\chi)} + (\overline{\chi(C)})e_{(c,\chi^{-1})} + (\overline{\chi(D)})e_{(d,\chi)}$

(2) $\nu_Q(e_{(b,\chi)}) = \overline{-\chi(B)}e_{(a,\chi)} + (4\lambda + 3 - \overline{\chi(A)})e_{(b,\chi)} - (\overline{\chi(D)})e_{(c,\chi)} + (\overline{\chi(C)})e_{(d,\chi^{-1})}$

(3) $\nu_Q(e_{(c,\chi)}) = \overline{-\chi(C)}e_{(a,\chi^{-1})} + (\chi(D))e_{(b,\chi)} + (4\lambda + 3 - \chi(A))e_{(c,\chi)} - (\chi(B))e_{(d,\chi)}$

(4) $\nu_Q(e_{(d,\chi)}) = -\chi(D)e_{(a,\chi)} - (\overline{\chi(C)})e_{(b,\chi^{-1})} + (\overline{\chi(B)})e_{(c,\chi)} + (4\lambda + 3 - \overline{\chi(A)})e_{(d,\chi)}$.

The result above follows by straightforward applications of the relations in (2) and Lemma 10.

Let χ_0 denote the trivial character of G. For $\chi \neq \chi_0 \in Irr(G)$, define N_χ to be the $\mathcal{R}^V$ submodule generated by $\{e_{(\mu,f)} | \, \mu = a, b, c, d$ and $f = \chi, \chi^{-1}\}$. Let N_{χ_0} be the submodule generated by $\{v_1, v_2, v_3, e_{(\mu,\chi_0)} | \, \mu = a, b, c, d\}$. Lemma 12 shows that $\nu_Q(N_\chi) \subset N_\chi$ for $\chi \neq \chi_0$. Lemma 12 implies $\nu_Q(N_{\chi_0}) \subset N_{\chi_0}$. By ν_χ we denote $\nu_Q|_{N_\chi}$.

For $\chi \neq \chi_0$, let Q_χ be the matrix representation of ν_χ with respect to the ordered basis $(e_{(\mu,\chi)} |\ \mu = a, b, c, d) \cup (e_{(\mu,\chi^{-1})} |\ \mu = a, b, c, d)$ (see (5)). By Lemma 12 we have $Tr(\nu_\chi) = 16\lambda + 12 - 2(\chi(A) + \chi(-A)) = 2(8\lambda + 7)$. The eigenvalues of Q_χ are elements of the set $\left\{0, \dfrac{8\lambda + 7 - \left(\sqrt{8\lambda + 7}\right) i}{2}, \dfrac{8\lambda + 7 + \left(\sqrt{8\lambda + 7}\right) i}{2}\right\}$ of eigenvalues of Q. As $Tr(Q_\chi) = 8\lambda + 7$, the eigenvalues of Q_χ are $\dfrac{8\lambda + 7 - \left(\sqrt{8\lambda + 7}\right) i}{2}$ and $\dfrac{8\lambda + 7 + \left(\sqrt{8\lambda + 7}\right) i}{2}$ and that $det(Q_\chi) = (8\lambda + 7)^4(2\lambda + 2)^4$.

$$
(5) \qquad Q_\chi = \begin{pmatrix}
4\lambda+3-\chi(A) & -\chi(B) & 0 & -\chi(D) & 0 & 0 & -\chi(C) & 0 \\
\overline{\chi(B)} & 4\lambda+3-\overline{\chi(A)} & \chi(D) & 0 & 0 & 0 & 0 & -\chi(C) \\
0 & -\overline{\chi(D)} & 4\lambda+3-\chi(A) & \overline{\chi(B)} & \overline{\chi(C)} & 0 & 0 & 0 \\
-\chi(D) & 0 & -\chi(B) & 4\lambda+3-\overline{\chi(A)} & 0 & \chi(C) & 0 & 0 \\
0 & 0 & -\overline{\chi(C)} & 0 & 4\lambda+3-\overline{\chi(A)} & -\overline{\chi(B)} & 0 & -\overline{\chi(D)} \\
0 & 0 & 0 & -\overline{\chi(C)} & \chi(B) & 4\lambda+3-\chi(A) & \overline{\chi(D)} & 0 \\
\chi(C) & 0 & 0 & 0 & 0 & -\chi(D) & 4\lambda+3-\overline{\chi(A)} & \chi(B) \\
0 & \overline{\chi(C)} & 0 & 0 & -\overline{\chi(D)} & 0 & -\overline{\chi(B)} & 4\lambda+3-\chi(A)
\end{pmatrix}.
$$

Straight forward computations show that $Q_\chi \overline{Q_\chi^\intercal} = sI$, where $s = |\chi(A)|^2 + |\chi(B)|^2 + |\chi(C)|^2 + |\chi(D)|^2$. As $det(Q_\chi) = (8\lambda + 7)^4(2\lambda + 2)^4$, we have $s = (8\lambda + 7)(2\lambda + 2)$.

Let m_1 be the minor of Q_χ associated to row indices $\{1, 3, 5, 7\}$ and columns indices $\{1, 3, 5, 7\}$. Let m_2 be the minor of Q_χ associated to row indices $\{1, 3, 5, 7\}$ and columns indices $\{2, 4, 7, 8\}$. Computations yield $m_1 = ((4\lambda + 3)^2 + (4\lambda + 3) + |\chi(A)|^2 + |\chi(C)|^2)^2$ and $m_2 = (|\chi(B)|^2 + |\chi(D)|^2)^2$. We see that $\sqrt{m_2} + \sqrt{m_1} = (4\lambda + 3)^2 + (4\lambda + 3) + (8\lambda + 7)(2\lambda + 2) = (4\lambda + 3)(4\lambda + 4) + (8\lambda + 7)(2\lambda + 2)$. As both $4\lambda + 4$ and $4\lambda + 3$ are coprime to $8\lambda + 7$, we see that $\mathfrak{p}$ does not divide m_1 and m_2 simultaneously. So there is at least one 4-minor of Q_χ that is not divisible by $\mathfrak{p}$. Applying Lemma 7 and $det(Q_\chi) = (8\lambda + 7)^4(2\lambda + 2)^4$ we can conclude that the SNF of Q_χ over $\mathcal{R}$ is of the form $\mathrm{diag}(1, 1, 1, 1, e_5, e_6, e_7, e_8)$, where $e_5 \mid e_6 \mid e_7 \mid e_8$ and $\nu_\mathfrak{p}(e_5e_6e_7e_8) = 4\nu_\mathfrak{p}(8\lambda + 7)$. As $Q_\chi \overline{Q_\chi^\intercal} = (8\lambda + 7)(2\lambda + 2)I$, we can conclude that $\nu_\mathfrak{p}(e_i) = \nu_\mathfrak{p}(8\lambda + 7)$ for $i = 5, 6, 7, 8$. This concludes the proof of Theorem 5.

7. Critical group of $\mathcal{P}(q)$.

We now turn our attention to Paley tournament graph $\mathcal{P}(q)$. The computation of critical group of $\mathcal{P}(q)$ is essentially the same as that of the Paley graph done in [5]. The proofs of results in this section are similar to those in [5].

Let $q = p^t$ be a power of a prime p with $q \equiv 3 \pmod 4$. Let K be the group field with q elements and let H be the subgroup of squared in $K^\times$. We recall that the Paley tournament graph $\mathcal{P}(q)$ is the Cayley graph of $(K, +)$ with "connection" set being H.

$\mathcal{P}(q)$ is a DRT with parameters $\left(q, k := \dfrac{q-1}{2}, \lambda := \dfrac{q-3}{4}\right)$. Let Q be the Laplacian matrix of $\mathcal{P}(q)$ and $\mathcal{K}$ be its critical group . By Theorem 3, we have $\mathcal{K} = (\mathbb{Z}/(\mu)\mathbb{Z})^{2\mu} \oplus \mathcal{K}_2$, where $\mu = \dfrac{q-1}{4}$ and $\mathcal{K}_2$ is the subgroup of order $q^{\frac{q-3}{2}}$. So we now need to determine the Sylow p-subgroup of $\mathcal{K}$. We do this by determining the SNF of Q over an unramified extension of $\mathbb{Z}_p$.

Let R be the ring of integers of the unique unramified extension of degree t over $\mathbb{Q}_p$. Then the ideal pR is a maximal ideal, and thus $K = R/pR \cong \mathbb{F}_q$. By R^K, we denote the free module over R generated by $\{[x] |\ x \in K\}$. The matrix Q defines a map $\nu_Q : R^K \to R^K$ that satisfies $\nu_Q([x]) = k[x] - \sum_{z\in S} [x + z]$. In other words Q is the matrix representation of ν_Q with respect to some ordering of the basis set $\{[x] |\ x \in K\}$.

Now H acts a group of automorphisms on $\mathcal{P}(q)$. So ν_Q is in fact an H-endomorphism of R^K.By $Irr(H)$ we denote the irreducible R-valued characters of H. Given $\chi \in Irr(H)$, we define $N_\chi := \{x \in \mathcal{R}^K | g.x = \chi(g)x \text{ for all } g \in H\}$. In other words, N_χ is the direct sum of all irreducible submodules of $\mathcal{R}^V$ that affording χ. As H preserves adjacency, ν_Q is an $\mathcal{R}H$ map. Now by applying Schur's Lemma, we have $\nu(N_\chi) \subset N_\chi$.

The action of H on R^K is the restriction of the natural action of $K^\times$ on R^K. Let $T : K^\times \to R^\times$ be the Teichmüller character generating the cyclic group $\mathrm{Hom}(K^\times, R^\times)$. Then $K^\times$ action on R^K decomposes it into the direct sum $R[0] \oplus R^{K^\times}$. Now the regular module $R^{K^\times}$ decompose further into a direct sum of $K^\times$-invariant submodules of rank 1, affording the characters T^i, $i = 0, \ldots, q-2$. The component affording T^i is spanned by $f_i := \sum_{x\in K^\times} T^i(x^{-1})[x]$. Therefore

$\{\mathbf{1}, f_1 \dots f_{q-2}, [0]\}$ is a basis for R^K, where $\mathbf{1} := f_0 + [0] = \sum_{x \in K} [x]$. The characters T^i and T^{-i} are the same when restricted to H. So we have (a)$Irr(H) = \{T^i | 0 \leq i \leq k = \frac{q-1}{2}\}$; for $1 \leq i < k$, we have $N_i := N_{T^i} = Rf_i + Rf_{i+k}$; and $N_0 := N_{T^0} = R[0] + Rf_k + R\mathbf{1}$. We now have $R^K = \bigoplus_{i=0}^{k-1} N_i$ with $\nu_Q(N_i) \subset N_i$ for all $0 \leq i \leq k-1$.

Following conventions in [1], we extend the T^i's to K. As per this convention, the character T^0 maps every element of K to 1, while T^{q-1} maps 0 to 0. All other characters map 0 to 0. For two integers a, b the Jacobi sum $J(T^a, T^b)$ is $\sum_{x \in K} T^a(x) T^b(1-x)$. We refer the reader to Chapter 2 of [3] for formal properties of Jacobi sums. Following the conventions established, for $a \not\equiv 0 \pmod{q-1}$, we have $J(T^a, T^0) = 0$ and $J(T^a, T^{q-1}) = -1$.

The following Lemma describes action of μ_Q on N_i. This result is essentially [5, Lemma 3.1].

Lemma 13. *(1) If $1 \leq i \leq k-1$, we have $\mu_Q(f_i) = \frac{1}{2}\left(qf_i - J(T^{-i}, T^k) f_{i+k}\right)$.*

(2) $\mu_Q(f_k) = \frac{1}{2}(-\mathbf{1} + qf_k + q[0])$.

(3) $\mu_Q([0]) = \frac{1}{2}(q[0] - f_k - \mathbf{1})$.

(4) $\mu_Q(\mathbf{1}) = 0$.

Proof. We observe that the characteristic function δ_H of H in K is $\frac{T^0 + \psi - \delta_{\{0\}}}{2}$, where $\psi = T^k$ is the quadratic character. We now recall that $\nu_Q([x]) = kx - \sum_{y \in Y} \delta_H(y)[x+y]$.

We have

$$\begin{aligned}
2\mu_Q(f_i) &= 2\sum_{x \in K^\times} T^{-i}(x)\mu_Q([x]) \\
&= (q-1)f_i - 2\sum_{x \in K^\times} T^{-i}(x) \sum_{y \in K} \delta_H(y)([x+y]) \\
&= (q-1)f_i + \sum_{x \in K^\times} T^{-i}(x) \sum_{y \in K} \left(\delta_0(y) - T^0(y) - \psi(y)\right)[x+y] \\
&= qf_i - \sum_{x \in K^\times} T^{-i}(x) \sum_{y \in K} T^0(y)[x+y] - \sum_{x \in K^\times} T^{-i}(x) \sum_{y \in K} T^k(y)[x+y]
\end{aligned}$$

(1) We assume $1 \leq i \leq k-1$. In this case, the middle sum in the above expression $\sum_{x \in K^\times} T^{-i}(x) \sum_{y \in K} T^0(y)[x+y] = \left(\sum_{x \in K^\times} T^{-i}(x)\right) \times \left(\sum_{z \in K} [z]\right)$. For $i \neq 0$, as T^i is a non-trivial character of $K^\times$ and thus $\sum_{x \in K^\times} T^{-i}(x) = 0$.

The last sum in the expression above is

$$\sum_{x \in K^\times} T^{-i}(x) \sum_{y \in K} \psi(y)[x+y] = \sum_{x \in K^\times} T^{-i}(x) \sum_{y \in K} \psi(y)[x+y] = \sum_{z \in K^\times} \sum_{x \in K^\times} T^{-i}(x)\psi(z-x)[z] + \sum_{x \in K^\times} T^{-i}(x)\psi(-x)[0].$$

For $z \neq 0$, using $T^{-i}(x)\psi(z-x) = T^{-i}(z)\psi(z)T^{-i}(x/z)\psi(1-(x/z))$, we have

$$\begin{aligned}
\sum_{z \in K^\times} \sum_{x \in K^\times} T^{-i}(x)\psi(z-x)[z] &= \sum_{x,z \in K^\times} T^{-i}(x/z)\psi(1-(x/z))T^{-i}(z)\psi(z)[z] \\
&= \sum_{w,z \in K^\times} T^{-i}(w)\psi(w)T^{-i-k}(z)[z] \\
&= J(T^{-i}, \psi) f_{i+k}.
\end{aligned}$$

We have $\sum_{x \in K^\times} T^{-i}(x)\psi(-x)[0] = \left(\sum_{x \in K^\times} T^{-i+k}(x)\right)\psi(-1)[0]$. As $i \neq k$, T^{-i+k} is non trivial and thus $\sum_{x \in K^\times} T^{-i+k}(x) = 0$. We have now proved (i).

The proof of (2) follows by essentially the same computation as above and using the fact that $J(\psi, \psi) = -\psi(-1) = 1$. Results (3) and (4) are straightforward. $\square$

Corollary 14. *The Laplacian Q is similar over R to a diagonal matrix with diagonal entries $J(T^i, T^k)$ for $1 \le i \le q-2$ and $i \ne k$, two ones and one zero.*

So computing the p-adic valuations of Jacobi sums will give us the p-elementary divisors of Q.

An integer a not divisible by $q-1$ has, when reduced modulo $q-1$, a unique p-digit expansion $a \equiv a_0 + a_1 p + \ldots + a_{t-1} p^{t-1} \pmod{q-1}$, where $0 \le a_i \le p-1$. We represent this expansion by the tuple of digits $(a_0, \ldots, a_i, \ldots, a_{t-1})$. By $s(a)$ we denote the sum $\sum a_i$. For example, 1 has the expansion $(1, \ldots, 0, \ldots 0)$ and $s(1) = 1$.

Applying Stickelberger's theorem on Gauss Sums [24] and the well know relation between Gauss and Jacobi sums we can deduce the following theorem.

Theorem 15. *Let q be a power of a prime p and let a and b be integers not divisible by $q-1$. If $a+b \not\equiv 0 \pmod{q-1}$, then we have*

$$v_p(J(T^{-a}, T^{-b})) = \frac{s(a) + s(b) - s(a+b)}{p-1}.$$

In other words, the p-adic valuation of $J(T^{-a}, T^{-b})$ is equal to the number of carries, when adding p-expansions of a and b modulo $q-1$.

The p-adic expansion of $k = \dfrac{q-1}{2}$ is $\sum_{i=0}^{t-1} \dfrac{p-1}{2} p^i$ and thus $s(k) = \dfrac{t(p-1)}{2}$. We have $v_p(J(T^{-i}, T^k)) = c(i) := \dfrac{s(i) + t(p-1)/2 - s(i+k)}{p-1}$. In other words, $c(i)$ is the number of carries when adding the p-adic expansions of i and k, modulo $q-1$. Observing that $c(i) + c(q-1-i) = t$, we see that $c(i) \le t$.

We need to solve the following problem in order to find the p-elementary divisors of Q.

Counting Problem: For $1 \le i \le q-2$ and $i \ne k$, by $c(i)$ we denote the number of carries when adding the p-adic expansions of i and k, modulo $q-1$. Given $0 \le a \le t$, find $e_a := |\{i | \, c(i) = a\}|$.

The multiplicity of p^a as an elementary divisor of Q is e_a. This counting problem was solved in [5, §4], using the p-ary add-with-carry algorithm [9, Theorem 4.1] and the transfer matrix method [21, Page 501]. [5, §4] contains the proof of the following Lemma which immediately shows Theorem 6.

Lemma 16. *(1)* $e_t = \left(\dfrac{p+1}{2}\right)^t - 2$*;*

(2) and for $1 \le i < t$,

$$e_i = \sum_{j=0}^{\min\{i,t-i\}} \frac{t}{t-j} \binom{t-j}{j} \binom{t-2j}{i-j} (-p)^j \left(\frac{p+1}{2}\right)^{t-2j}.$$

Acknowledgement

I thank Prof. Peter Sin for his valuable suggestions and feedback.

References

[1] James Ax. Zeroes of polynomials over finite fields. *American Journal of Mathematics*, 86(2):255–261, 1964.

[2] Hua Bai. On the critical group of the n-cube. *Linear algebra and its applications*, 369:251–261, 2003.

[3] Bruce C Berndt, Kenneth S Williams, and Ronald J Evans. *Gauss and Jacobi sums*. Wiley, 1998.

[4] Andries Brouwer, Joshua Ducey, and Peter Sin. The elementary divisors of the incidence matrix of skew lines in PG$(3, q)$. *Proceedings of the American Mathematical Society*, 140(8):2561–2573, 2012.

[5] David B. Chandler, Peter Sin, and Qing Xiang. The Smith and critical groups of Paley graphs. *Journal of Algebraic Combinatorics*, 41(4):1013–1022, Jun 2015.

[6] Cunsheng Ding, Zeying Wang, and Qing Xiang. Skew Hadamard difference sets from the ReeTits slice symplectic spreads in pg(3,32h+1). *Journal of Combinatorial Theory, Series A*, 114(5):867 – 887, 2007.

[7] Cunsheng Ding and Jin Yuan. A family of skew Hadamard difference sets. *Journal of Combinatorial Theory, Series A*, 113(7):1526 – 1535, 2006.

[8] Joshua E Ducey, Jonathan Gerhard, and Noah Watson. The smith and critical groups of the square rook's graph and its complement. *arXiv preprint arXiv:1507.06583*, 2015.

[9] Tor Helleseth, Henk DL Hollmann, Alexander Kholosha, Zeying Wang, and Qing Xiang. Proofs of two conjectures on ternary weakly regular bent functions. *IEEE Transactions on Information Theory*, 55(11):5272–5283, 2009.

[10] Brian Jacobson, Andrew Niedermaier, and Victor Reiner. Critical groups for complete multipartite graphs and cartesian products of complete graphs. *Journal of Graph Theory*, 44(3):231–250, 2003.

[11] H. Kharaghani and B. Tayfeh-Rezaie. A Hadamard matrix of order 428. *Journal of Combinatorial Designs*, 13(6):435–440, 2005.

[12] Dino Lorenzini. Smith normal form and Laplacians. *Journal of Combinatorial Theory, Series B*, 98(6):1271 – 1300, 2008.
[13] Dino J Lorenzini. A finite group attached to the Laplacian of a graph. *Discrete Mathematics*, 91(3):277–282, 1991.
[14] T. S. Michael and W. D. Wallis. Skew-Hadamard matrices and the Smith normal form. *Designs, Codes and Cryptography*, 13(2):173–176, Feb 1998.
[15] Koji Momihara and Qing Xiang. Constructions of skew Hadamard difference families. *European Journal of Combinatorics*, 76:73 – 81, 2019.
[16] Morris Newman. On the Smith normal form. *J. Res. Nat. Bur. Standards Sect. B*, 75:81–84, 1971.
[17] R. E. A. C. Paley. On orthogonal matrices. *Journal of Mathematics and Physics*, 12(1-4):311–320, 1933.
[18] Venkata Raghu Tej Pantangi. Critical group of van Lint-Schrijver cyclotomic strongly regular graphs. *To appear in Finite fields and their applications*, 2019.
[19] Venkata Raghu Tej Pantangi and Peter Sin. Smith and critical groups of polar graphs. *arXiv preprint arXiv:1706.08175*, 2017.
[20] K.B Reid and Ezra Brown. Doubly regular tournaments are equivalent to skew Hadamard matrices. *Journal of Combinatorial Theory, Series A*, 12(3):332 – 338, 1972.
[21] Richard P. Stanley. *Enumerative Combinatorics: Volume 1*. Cambridge University Press, New York, NY, USA, 2nd edition, 2011.
[22] Richard P. Stanley. *Enumerative Combinatorics: Volume 2*. Cambridge University Press, New York, NY, USA, 2nd edition, 2011.
[23] Richard P Stanley. Smith normal form in combinatorics. *Journal of Combinatorial Theory, Series A*, 144:476–495, 2016.
[24] L. Stickelberger. Ueber eine verallgemeinerung der Kreistheilung. *Mathematische Annalen*, 37(3):321–367, Sep 1890.
[25] G Szekeres. Tournaments and Hadamard matrices. *Enseignement Math*, 15(2):269–278, 1969.
[26] G. Szekeres. Cyclotomy and complementary difference sets. *Acta Arithmetica*, 18(1):349–353, 1971.
[27] A. Vince. Elementary divisors of graphs and matroids. *European Journal of Combinatorics*, 12(5):445 – 453, 1991.
[28] Jennifer Wallis and Albert Leon Whiteman. Some classes of Hadamard matrices with constant diagonal. *Bulletin of the Australian Mathematical Society*, 7(2):233249, 1972.
[29] Albert Leon Whiteman. An infinite family of skew Hadamard matrices. *Pacific J. Math.*, 38(3):817–822, 1971.

Email address: `pvrt1990@gmail.com`