CRITICAL GROUPS OF VAN LINT-SCHRIJVER CYCLOTOMIC STRONGLY REGULAR GRAPHS.

VENKATA RAGHU TEJ PANTANGI

Abstract. The *critical* group of a finite connected graph is an abelian group defined by the Smith normal form of its Laplacian. Let q be a power of a prime and H be a multiplicative subgroup of $K = \mathbb{F}_q$. By $\mathrm{Cay}(K, H)$ we denote the Cayley graph on the additive group of K with "connection" set H. A strongly regular graph of the form $\mathrm{Cay}(K, H)$ is called a *cyclotomic strongly regular graph*. Let p and $\ell > 2$ be primes such that p is primitive $\pmod{\ell}$. We compute the *critical* groups of a family of *cyclotomic strongly regular graphs* for which $q = p^{(\ell-1)t}$ (with $t \in \mathbb{N}$) and H is the unique multiplicative subgroup of order $k = \frac{q-1}{\ell}$. These graphs were first discovered by van Lint and Schrijver in [22].

1. Introduction

Let $\Gamma = (V, E)$ be a finite, simple, and connected graph. Let A be the adjacency matrix of Γ with respect to some arbitrary but fixed ordering of the vertex set V. Define the matrix D to be the diagonal matrix of size $|V|$ whose ith diagonal entry is the valency of the ith vertex of Γ. The matrix $L := D - A$ is called the Laplacian matrix of Γ. By $\mathbb{Z}V$ we denote the free $\mathbb{Z}$ module with V as a basis set. By abuse of notation, we may consider L to be an element of $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}V)$. The *critical* group $C(\Gamma)$ is the torsion of the cokernal of L.

These groups are invariants of Γ. By Kirchhoff's Matrix-tree theorem, it may be deduced that the order of $C(\Gamma)$ is equal to the number of spanning trees of Γ (for eg. see [20]). The *critical* group arises as the *abelian sandpile group* in statistical physics (cf. [9]). This group appears arises in graph theory in the context of the chip firing game (cf. [4]). An early author on the *critical* group was Vince, who in [23] computed them for Wheel graphs and complete bipartite graphs. In the same paper, it was shown that the group depends only on the cycle matroid of the graph. Other papers that include computation of *critical* groups of families of graphs include [8], [2], [14], [10], [6], and [16]. In [15], Lorenzini examined the proportion of graphs with cyclic *critical* groups among graphs with *critical* groups of particular order. There are relatively few classes of graphs with known *critical* groups. A particular class of groups that proved amenable to computations is the class of strongly regular graphs (for eg. see [8]). In this paper we describe the critical groups of the *cyclotomic strongly regular graphs* discovered in [22].

Consider a finite field K of characteristic p and a subgroup H of K^*. By $\mathrm{Cay}(K, H)$ we denote the Cayley graph on the additive group of K with connection set H. If $\mathrm{Cay}(K, H)$ is a strongly regular graph, then we speak of a *cyclotomic strongly regular graph* (*cyclotomic SRG*). The Paley graph is a well known example of a *cyclotomic SRG*. Extensive scholarship on these graphs include [22], [5], [17], and [12]. We refer the reader to section 4 of [24] for a survey on these graphs. If H is the multiplicative group of a non-trivial subfield of K, then $\mathrm{Cay}(K, H)$ is a *cyclotomic SRG*. A graph of this form is called a *subfield cyclotomic SRG*. Other examples of *cyclotomic SRGs* are the *semi-primitive cyclotomic SRGs*. Consider a subgroup H of K^* with $N = [K^* : H] > 1$ and $N \mid \frac{|K^*|}{p-1}$. Further assume that there exists an integer s such that $p^s \equiv -1 \pmod{N}$. These arithmetic restrictions on H ensure that the adjacency matrix of the regular graph $\mathrm{Cay}(K, H)$ has exactly 3 eigenvalues and thus is a *cyclotomic SRG* (see for example Section 4 of [24]). A graph of this form is called a *semi-primitive cyclotomic SRG*. According to a conjecture by Schmidt and White (Conjecture 4.4 of [17]/ Conjecture 4.1 of [24]), other than the above mentioned classes, there are only 11 sporadic examples of *cyclotomic SRG*. In this paper we consider a class of *semi-primitve cyclotomic SRGs* discovered in [22].

Consider primes p, $\ell \neq 2$ and $t \in \mathbb{N}$. The graph $G(p, \ell, t)$ denotes $\mathrm{Cay}(K, S)$, where $K = \mathbb{F}_{p^{(\ell-1)t}}$ and S is the subgroup of index ℓ in K^* . Further assume a) $p^{(\ell-1)t/2} \neq \ell - 1$ whenever t is odd; and b)p is primitive in $\mathbb{Z}/\ell\mathbb{Z}$. The arithmetic constraint a) is equivalent to the graph being connected, and b) implies that $G(p, \ell, t)$ is a *semi-primitive SRG*. These *semi-primitive cylclotomic SRGs* were discovered in [22]. In this paper we describe the *critical* groups of this family of graphs. The construction of this family is similar to that of Paley and Piesert graphs. The *critical* group

Key words and phrases. invariant factors, elementary divisors, Smith normal form, critical group, sandpile group, adjacency matrix, Laplacian, Cyclotomy.

of the Paley graph was computed in [8], and that of Piesert was described in [18]. We extend the techniques used in [8] and [18] to compute the *critical* group of $G(p, \ell, t)$ (with (p, ℓ, t) satisfying arithmetic constraints a) and b)).

We denote the critical group of $G(p, \ell, t)$ by C. Theorem 3 describes the p-complementary part of C. We apply a standard method of diagonalizing the Laplacian using the character table of $\mathbb{F}_q$ (here $q = p^{(\ell-1)t}$). A different approach is required to obtain a description of the p-part of C. In §6, we study the permutation action of S on R-free module $R\mathbb{F}_q$ with basis $\mathbb{F}_q$, where R is the ring of integers of a suitable extension of $\mathbb{Q}_p$. Let $\hat{S}$ be the set of R valued characters of S. We obtained the decomposition $R\mathbb{F}_q = \bigoplus_{\chi\in\hat{S}} N_\chi$, where N_χ is the isotypic component of the S module $R\mathbb{F}_q$ corresponding to the character χ. Since S preserves adjacency, each of these isotypic components is invariant under the Laplacian L. Some Jacobi sums naturally arise in the computation of the Smith normal form of L restricted to these isotypic components. The description of the p-part of C is reduced to computation of p-adic valuations of Jacobi sums. The main problem is now reduced to computing the p-adic valuations of certain Jacobi sums. Classical results by Stickelberger and Gauss describe the p-adic valuations of Jacobi sums in combinatorial terms. Theorem 1 gives a description of the p-part in terms of p-adic valuations of Jacobi sums. Writing the elementary divisor form of C is now reduced to a counting problem. We were able to use the transfer matrix method to determine the elementary divisor form in the case $\ell = 3$. For a fixed t, Theorem 2 leads to a recursive algorithm that yields the p-elementary divisors of the *critical* group of the family of graphs $G(p, 3, t)$, where p runs over all primes p with $p \equiv 2 \pmod 3$. We were not able to obtain a similar result in the case $\ell \neq 3$. As a consequence we were able to show that the p-rank of the Laplacian of $G(p, 3, t)$ is $\left(\frac{p+1}{3}\right)^{2t}(2^{t+1} - 2)$ (see Cor. 14).

2. Definitions and Notation.

Let p and $\ell > 2$ be primes, with p being primitive $\pmod \ell$. Let $t \in \mathbb{N}$ and $q = p^{(\ell-1)t}$. Moreover assume that $\sqrt{q} = p^{(\ell-1)t/2} \neq \ell - 1$ whenever t is odd. Consider the field $K = \mathbb{F}_q$ and S be the unique subgroup of K^* of order $k := (q-1)/\ell$. Then by $G(p, \ell, t)$ we denote the graph with vertex set K and edge set $\{\{x, y\} \mid x, y \in K \text{ and } x - y \in S\}$. This is the undirected Cayley graph associated with (K, S). By A we denote the adjacency matrix of $G(p, \ell, t)$ with respect to some fixed but arbitrary ordering of the vertex set K. The Laplacian matrix is denoted by L. By C, we mean the critical group of $G(p, \ell, t)$.

Given a prime and an integer a, throughout the paper $v_p(a)$ denotes the p-adic valuation of a.

3. Some properties of $G(p, \ell, t)$.

It was shown in section 2 of [22] that $G(p, \ell, t)$ is a strongly regular graph with parameters

$$\left(q,\ \frac{q-1}{\ell},\ \frac{q - 3\ell + 1 + (-1)^{t+1}(\ell-1)(\ell-2)\sqrt{q}}{\ell^2},\ \frac{q - \ell + 1 + (-1)^t(\ell-2)\sqrt{q}}{\ell^2}\right),$$

where $q = p^{(\ell-1)t}$. Let χ_1 denote the Teichmller character of the additive group of K. Given $a \in K$, let χ_a denote the additive character satisfying $\chi_a(x) = \chi_1(ax)$ for all $x \in K$. Given an additive character χ of K define $r_\chi = \sum_{x\in S} \chi(s)$. Lemma 2 of [22] shows that $\sum_{x\in K} \chi(x)x$ is an eigenvector for the adjacency matrix A of $G(p, \ell, t)$ with eigenvalue r_χ.

By the discussion that follows Lemma 2 in [22], the adjacency matrix A of Γ has eigenvalues k, r_{χ_1}, r_{χ_α} with multiplicities 1, k, and $q - k - 1$ respectively. Here α is a generator of K^*. It was also shown that $r_{\chi_\alpha} = \frac{-1 + (-1)^t\sqrt{q}}{\ell}$, and $r_{\chi_1} = r_{\chi_\alpha} + (-1)^{t+1}\sqrt{q}$. Thus the eigenvalues of the Laplacian L are 0, $u = k - r_{\chi_1}$ and $v = k - r_{\chi_\alpha}$, with multiplicities 0, k, and $q - k - 1$ respectively. We can see that $v = \sqrt{q}\frac{\sqrt{q} + (-1)^{t+1}}{\ell}$, and $u = v + (-1)^t\sqrt{q}$. It is well known that the nullity of the Laplacian matrix of a graph is equal to the number of connected components. Clearly $v \neq 0$, and thus $G(p, \ell, t)$ is connected if and only if either t is even or t is odd and $\sqrt{q} \neq \ell - 1$. We will assume throughout that $p^{(\ell-1)t/2} \neq \ell - 1$ whenever t is odd.

Let $v_p(\ell - 1) = d$, then $v_p(u) = \frac{1}{2}(\ell-1)t + d$ and $v_p(v) = \frac{1}{2}(\ell-1)t$.

By Theorem 8.1.2 of [7], we have

$$L(L - (v + u)I) = vuI + \mu J. \tag{3.1}$$

4. Main Results

Let p and $\ell \neq 2$ be a primes with p primitive modulo ℓ. Given $t \in \mathbb{N}$, let $q = p^{(\ell-1)t}$ and $k = \dfrac{q-1}{\ell}$. The following theorem describes the Sylow p-subgroup C_p of the critical group C of $G(p, \ell, t)$.

Theorem 1. *Consider the graph $G(p, \ell, t)$ with $\sqrt{q} = p^{(\ell-1)t/2} \neq \ell - 1$ whenever t is odd. Let d be $v_p(\ell - 1)$. Given integers a, b not divisible by $q-1$, let $c(a, b)$ denote the number of carries when adding the p-adic expansions of a and $b \pmod{q-1}$. Let L be the Laplacian matrix and C be the* critical *group of $G(p, \ell, t)$. For $1 \leq i < k-1$, let*

$$c(i) = \min\left(\{c(i + mk, nk) | 0 \leq m \leq \ell - 1 \text{ and } 0 \leq n \leq \ell - 1\}\right).$$

Given a non-zero positive integer j, let e_j be the multiplicity of p^j as a p-elementary divisor of C. By e_0 we denote the p-rank of the Laplacian L of $G(p, \ell, t)$. Then we have the following.

(1) $e_0 = |\{i \mid 1 \leq i \leq k-1 \text{ and } c(i) = 0\}| + 2$ *and* $e_{(\ell-1)t+d} = e_0 = |\{i \mid c(i) = 0\}|$.
(2) $e_j = |\{i \mid 1 \leq i \leq k-1 \text{ and } c(i) = j\}|$ *for* $0 < j < \frac{(\ell-1)t}{2}$.
(3) $e_j = e_{(\ell-1)t+d-j}$ *for* $0 < j < \frac{(\ell-1)t}{2}$.
(4) *If* $p \nmid \ell - 1$, *then* $e_{\frac{(\ell-1)t}{2}} = q + 1 - 2\sum\limits_{j<t} e_j$.
(5) *If* $p \mid \ell - 1$, *then*
  (a) $e_{\frac{(\ell-1)t}{2}+d} = k + 2 - \sum\limits_{j<t} e_j$ *and*
  (b) $e_{\frac{(\ell-1)t}{2}} = (\ell - 1)k - \sum\limits_{j<t} e_j$.
(6) $e_j = 0$ *for all other* j.

We prove the above Theorem in §7.

In the case of $G(p, 3, t)$, using the transfer matrix method (cf. Section 4.7 of [19]) we were able to determine a closed form for the p-rank (i.e e_0 in the context of the Theorem above) of the Laplacian. The following theorem gives a quick recursive algorithm to compute other p-elementary divisors. The proof of the following result is in §8.

Let $P = \left(\left(\frac{p+1}{3}\right)^2 (x^2y^2 + x^2y + xy^2 + x + y + 1) + \left(\frac{p-2}{3}\right)^2 3xy\right)$, $R = p^2x^3y^3$ and

$Q = \left(\left(\frac{p+1}{3}\right)^2 (xy)(x^2y^2 + x^2y + xy^2 + x + y + 1) + \left(\frac{2p-1}{3}\right)^2 3x^2y^2\right)$. We define the polynomial $C(2t) \in \mathbb{C}[x, y]$ recursively as follows:

$$\begin{aligned} C(2) &= 2P \\ C(4) &= 2(P^2 - 2Q), \\ C(6) &= 6R + 2(P^3 - 2QP) - 2PQ, \\ \text{and } C(2t) &= PC(2t-2) - QC(2t-4) + RC(2t-6) \text{ for } t > 3. \end{aligned} \tag{4.1}$$

Theorem 2. *Let C_p be the Sylow p-subgroup of the critical group of the graph $G(p, 3, t)$ (with $(p, t) \neq (2, 1)$). Given a non-zero positive integer j, let e_j be the multiplicity of p^j as a p-elementary divisor of C. By e_0 we denote the p-rank of the Laplacian L of $G(p, 3, t)$. Let E_{ab} be the coefficient of x^ay^b in $C(2t)$. Then we have the following (Here δ_{ij} is the Kronecker delta function.).*

(1) $e_0 = e_{2t+\delta_{2,p}} + 2 = \left(\frac{(p+1)}{3}\right)^{2t} (2^{t+1} - 2)$.
(2) *For $a < t$, we have* $e_a = e_{2t+\delta_{2,p}-a} = \sum\limits_{a<b\leq t} E_{ab}$
(3) $e_{t+\delta_{2,p}} = (k + 2 - \sum\limits_{j<t} e_j) + (1 - \delta_{2,p})(2k - \sum\limits_{j<t} e_j)$.
(4) $e_t = (1 - \delta_{2,p})(k + 2 - \sum\limits_{j<t} e_j) + (2k - \sum\limits_{j<t} e_j)$.
(5) $e_a = 0$ *for all other* a.

Let X be the complex character table of $\mathbb{F}_q$ and A the adjacency matrix of $G(p, \ell, t)$. Then all the entries of X lie in $\mathbb{Z}[\zeta]$ for some primitive pth root of unity ζ. We have character orthogonality $\dfrac{1}{q}XX^t = I$ and

$$\frac{1}{q}XAX^t = \operatorname{diag}(r_\psi)_\psi, \tag{4.2}$$

where ψ runs over additive characters of $\mathbb{F}_q$ and r_ψ is as defined in §3. Note that r_ψ is an eigenvalue of A. We can now conclude that L is similar to $\mathrm{diag}(0, \underbrace{u \ \dots \ u}_{k \text{ times}}, \underbrace{v \ \dots \ v}_{q-k-1 \text{ times}})$, over $\mathbb{Z}[\zeta]$. We have now proved the following result.

Theorem 3. *Consider the graph $G(p,\ell,t)$ with $p^{(\ell-1)t/2} \neq \ell - 1$. Then the p-part of the* critical *group is $C_{p'} \cong \left(\frac{\mathbb{Z}}{u'\mathbb{Z}}\right)^k \times \left(\frac{\mathbb{Z}}{v'\mathbb{Z}}\right)^{q-k-1}$. Here v' is the biggest divisor of $\sqrt{q}\frac{\sqrt{q}+(-1)^{t+1}}{\ell}$ that is coprime to p, and u' is the biggest divisor of $u = v + (-1)^t\sqrt{q}$ that is coprime to p.*

Example 1. Implementing the Recursion in 4.1 in a computer algebra system such as Sage, we can compute $C(8)$. Now application of Theorems 2 and 3 yield the *critical* groups of the family of graphs $(G(p,3,4))_p$, with p running over primes primitive $\pmod 3$.

The 2-part of the *critical* group of $G(2,3,4)$ is $\prod_{i=1}^{9}\left(\frac{\mathbb{Z}}{2^i\mathbb{Z}}\right)^{e_i}$, where $[e_i]_{i=1}^9 = [32, 8, 16, 84, 1, 16, 8, 32, 28]$. The 2-complement of the *critical* group of $G(2,3,4)$ is $\mathbb{Z}/15\mathbb{Z}$.

The p-part of the *critical* group of $G(p,3,4)$ (with $p \neq 2$) $\prod_{i=1}^{8}\left(\frac{\mathbb{Z}}{p^i\mathbb{Z}}\right)^{e_i(p)}$, where

(1) $e_8(p) = 510\left(\frac{(p+1)}{3}\right)^8 - 2$,
(2) $e_1(p) = e_7(p) = 256/6561p^8 + 1040/6561p^7 + 1120/6561p^6 - 784/6561p^5 - 2240/6561p^4 - 784/6561p^3 + 1120/6561p^2 + 1040/6561p + 256/6561$,
(3) $e_2(p) = e_6(p) = 776/6561p^8 + 592/6561p^7 - 2248/6561p^6 - 1904/6561p^5 + 320/6561p^4 - 1904/6561p^3 - 2248/6561p^2 + 592/6561p + 776/6561$,
(4) $e_3(p) = e_5(p) = 304/2187p^8 - 448/2187p^7 - 128/2187p^6 + 608/2187p^5 - 32/2187p^4 + 608/2187p^3 - 128/2187p^2 - 448/2187p + 304/2187$,
(5) and $e_4(p) = 871/2187p^8 - 352/2187p^7 + 448/2187p^6 - 544/2187p^5 - 56/2187p^4 - 544/2187p^3 + 448/2187p^2 - 352/2187p + 871/2187$.

The p-complement of the *critical* group of $G(p,3,4)$ (with $p \neq 2$) is $\mathbb{Z}/u'v'\mathbb{Z}$,where $u' = \frac{p^4-1}{3}$ and $v' = \frac{p^4+2}{3}$.

Remark. For a fixed t, Theorem 2 implies that the multiplicities of the p-elementary divisors of the Laplacian of $G(p,3,t)$ are polynomial expressions in p of degree $2t$. We were however unable to extend the techniques in §8 to prove similar results in the general case.

5. Smith normal form

Let R be a Principal Ideal Domain and $T : R^m \to R^n$ be a linear transformation. By the structure theorem of finitely generated modules over PIDs, we have $\{\alpha_i\}_{i=1}^s \subset R \setminus \{0\}$ such that $\alpha_i \mid \alpha_{i+1}$ and

$$\mathrm{coker}(T) \cong R^{n-s} \oplus \bigoplus_{i=1}^{s} R/\alpha_i R.$$

With some abuse of notation we denote the matrix of the linear transformation T with respect to standard bases by T. Then the above equation tells us that we can find $P \in \mathrm{GL}_n(R)$, and $Q \in \mathrm{GL}_m(R)$ such that

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

where $Y = \mathrm{diag}(\alpha_1 \dots \alpha_s)$. The diagonal form PTQ is called the Smith normal form of T. Its uniqueness (up to multiplication of α_i by units) is also guaranteed by the aforementioned structure theorem.

The following is well known result (for eg. see Theorem 2.4 of [20]) that gives a description of the Smith normal form in terms of minor determinants.

Lemma 4. *Let T and $\{\alpha_i\}_{1\le i\le s}$ be as described above. Given $1 \le i \le s$, let $d_i(T)$ be the GCD of all $i \times i$ minor determinants of T, and let $d_0(T) = 1$. We then have $\alpha_i = d_i(T)/d_{i-1}(T)$.*

Let $\mathsf{p} \in R$ be a prime dividing α_r. Define $e_j(\mathsf{p}) = |\{\alpha_i | \ v_{\mathsf{p}}(\alpha_i) = j\}|$. Now e_j is the multiplicities of p^j as a p-elementary divisors of $\operatorname{coker}(T)$. If $R = \mathbb{Z}$, then $e_j(\mathsf{p})$ is the multiplicity of $\mathbb{Z}/\mathsf{p}^j\mathbb{Z}$ in the elementary divisor representation of the abelian group $\operatorname{coker}(T)$.

Let R_{p} be the p-adic completion of R. We have

$$R_{\mathsf{p}}^n/T(R_{\mathsf{p}}^m) \equiv R_{\mathsf{p}}^{n-s} \oplus \bigoplus_{j>0} \left(R_{\mathsf{p}}/\mathsf{p}^j R_{\mathsf{p}}\right)^{e_j(\mathsf{p})}.$$

Define $M_j(T) := \{x \in R^m | \ T(x) \in \mathsf{p}^j R_{\mathsf{p}}^n\}$. For ease of notation, we denote $M_j(T)$ by M_j and $e_j(\mathsf{p})$ by e_j. We have $R^m = M_0(T) \supset M_1(T) \supset \ldots \supset M_n(T) \supset \cdots$.

Let $\mathbb{F} = R_{\mathsf{p}}/\mathsf{p}R_{\mathsf{p}}$. If $M \subset R^m$ is a submodule, define $\overline{M} = (M + \mathsf{p}R_{\mathsf{p}}^m)/\mathsf{p}R_{\mathsf{p}}^m$.Then $\overline{M}$ is an $\mathbb{F}$-vector space. The following Lemma follows from the structure theorem.

Lemma 5. $e_j := \dim(\overline{M_j(T)}/\overline{M_{j+1}(T)})$.

So we have,

$$\dim(\overline{M_j(T)}) - \dim(\overline{\ker(T)}) = \sum_{t \geq j} e_t. \tag{5.1}$$

The following is Lemma 3.1 of [11].

Lemma 6. *Let C be an $n \times m$ integer matrix with $g = |Tor(\mathbb{Z}^n/C(\mathbb{Z}^m))|$. Fix a prime p and let $d = v_p(g)$. Let $M_i := M_i(C)$ be as defined above and $e_i := e_i(p)$ be the p-elementary divisors of C. If we have $0 < t_1 < t_2 \ldots < t_z$ and $s_1 > s_2 \ldots > s_n > s_{z+1} = \dim(\overline{\ker(C)})$ such that:*

1. $\dim(\overline{M_{t_i}}) \geq s_i$ *for* $1 \leq i \leq n$
2. $d = \sum_{i=1}^{n} (s_i - s_{i+1}) t_i$,

then

1. $e_0 = m - s_1$
2. $e_{t_i} = s_i - s_{i+1}$
3. $e_j = 0$ *for* $j \notin \{t_1 \ldots t_i, \ldots t_z\}$.

Proof. We have

$$\begin{aligned}
d &= \sum_{i \geq 1} i e_i \\
&\geq \sum_{k=1}^{r-1} \left(\sum_{a_k \leq i < a_{k+1}} i e_i \right) + \sum_{i \geq a_r} i e_i \\
&\geq \sum_{k=1}^{r-1} \left(a_k \sum_{a_k \leq i < a_{k+1}} e_i \right) + a_r \sum_{i \geq a_r} e_i \\
&\text{by (5.1) we have} \\
&= \sum_{k=1}^{r-1} \left(a_k (\dim(\overline{M_{a_k}}) - \dim(\overline{M_{a_{k+1}}})) \right) + a_r (\dim(\overline{M_{a_r}}) - \dim(\overline{\ker(C)})) \\
&\geq \sum_{i=1}^{r} (s_i - s_{i+1}) t_i \\
&= d.
\end{aligned}$$

So we have equality throughout. The results follow. □

Lemma 7 (12.8.4 of [7])**.** *Let C, be an $n \times n$ integer matrix with an integer eigenvalue ϕ of multiplicity c. Fix a prime p, dividing both $|Tor(\mathbb{Z}^n/C(\mathbb{Z}^n))|$ and ϕ, with $v_p(\phi) = d$. Then $\dim(\overline{M_d}(C)) \geq c$.*

Proof. Let V_ϕ be the eigenspace of $\mathbb{Q}_p^n$. Then $V_\phi \cap \mathbb{Z}_p^n$ is a pure $\mathbb{Z}_p$-submodule ($\mathbb{Z}_p$-direct summand) of $\mathbb{Z}_p^n$ of rank c. It is clear that $V_\phi \cap \mathbb{Z}_p^n \subset M_d(C)$. As $V_\phi \cap \mathbb{Z}_p^n$ is pure, we have $\overline{V_\phi \cap \mathbb{Z}_p^n} \subset \overline{M_d(C)}$. □

6. Character sums and block diagonal form of L.

As in §3, let p and $\ell > 2$ be primes, with p being primitive $\pmod{\ell}$. Let $t \in \mathbb{N}$ and $q = p^{(\ell-1)t}$. Moreover assume that $\sqrt{q} = p^{(\ell-1)t/2} \neq \ell - 1$ whenever t is odd. Consider the field $K = \mathbb{F}_q$ and S the unique subgroup of K^* of order $k := (q-1)/\ell$. Then by $G(p, \ell, t)$ we denote the graph with vertex set K and edge set $\{\{x, y\} \mid x, y \in K \text{ and } x - y \in S\}$. This is the undirected Cayley graph associated with (K, S).

By A we denote the adjacency matrix of $G(p, \ell, t)$ with respect to some fixed but arbitrary ordering of the vertex set K. The Laplacian matrix is denoted by L. By C, we mean the critical group of $G(p, \ell, t)$. We saw in §3 that L has eigenvalues 0, $v = \sqrt{q}\dfrac{\sqrt{q} + (-1)^{t+1}}{\ell}$ and $u = v + (-1)^t \sqrt{q}$, with multiplicities 1, $q - k - 1$ and k respectively.

Let R be the ring of integers of the unique unramified extension of degree $(\ell-1)t$ over $\mathbb{Q}_p$. Observe that $R/pR \cong \mathbb{F}_q = K$. Let R^K denote the free R-module with elements of K as a basis. Given $x \in K$, by $[x]$ we denote the element of R^K corresponding to x. Let T be the Teichmller character of the multiplicative group K^*. For $i \in \{0, 1, \ldots, q-2\}$ define $f_i := \sum_{x \in K^*} T^i(x^{-1})[x]$. Then $\{f_0, f_1 \ldots f_{q-2}, [0]\}$ is a basis for R^K.

Given an R-free RS-module M and a character $\chi : S \to R^*$, the isotypic component of M corresponding to χ is the RS-submodule $M_\chi := \{m \in M \mid sm = \chi(s)m \text{ for all } s \in S\}$. For $0 < j \leq k-1$, let N_j denote the R-submodule of R^K with basis $\{f_{i+mk} \mid 0 \leq m \leq \ell - 1\}$. Define N_0 to be the R-submodule with basis $\{\mathbf{1}, [0], f_k, \ldots f_{(\ell-1)k}\}$. Then N_i is the isotypic component for the character $T^i|_S$ of the group S. We also have

$$R^K = N_0 \oplus N_1 \ldots \oplus N_{k-1}. \tag{6.1}$$

We may view A and L as endomorphisms of R^K, with $A([x]) = \sum_{s \in S}[x+s],\ x \in K$ and $L([x]) = k[x] - \sum_{s \in S}[x+s],\ x \in K$.

Since S is a group of automorphisms for $G(p, \ell, t)$, the maps A and L are RS-module endomorphisms. It follows that A and L preserve the decomposition (6.1). Let L_i denote the matrix of $L|_{N_i}$ with respect to the basis $\{f_{i+mk} \mid 0 \leq m \leq \ell - 1\}$. So with respect to the basis $\{\mathbf{1}, [0], f_k, \ldots f_{(\ell-1)k}\}$, the matrix of L is $\operatorname{diag}(L_0, L_1, \ldots, L_{k-1})$. Determining the Smith normal forms of each of these blocks will determine the *critical* group.

Following conventions in [1], we extend the T^i's to $\mathbb{F}_q$. As per this convention, the character T^0 maps every element of $\mathbb{F}_q$ 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 $\sum_{x \in \mathbb{F}_q} T^a(x)T^b(1-x)$. We refer the reader to Chapter 2 of [3] for formal properties of Jacobi sums.

The following Lemma describes action of L_i on N_i.

Lemma 8. (1) *If $k \nmid i$, we have* $L(f_i) = \dfrac{1}{\ell}\left(qf_i - \sum_{m=1}^{\ell-1} J(T^{-i}, T^{-mk})f_{i+mk}\right)$.

(2) *If $0 \neq i = jk$, we have* $L(f_{jk}) = \dfrac{1}{\ell}\left(\mathbf{1} + qf_{jk} - \sum_{m \neq -j, 0} J(T^{-jk}, T^{-mk})f_{jk+mk} - q[0]\right)$.

(3) $L([0]) = \dfrac{1}{\ell}\left(q[0] - \sum_{m=1}^{\ell-1} f_{mk} - \mathbf{1}\right)$.

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

Proof. Let δ_S denote the characteristic function of S. We can observe that $\delta_S = \dfrac{1}{\ell}\left(\sum_{m=0}^{\ell-1} T^{mk} - \delta_0\right)$. Here δ_0 is 1 at 0 and 0 at all other field elements.

We have

$$
\begin{aligned}
A(f_i) &= \sum_{x\in K^*} T^i(x^{-1}) \sum_{y\in S}[x+y] \\
&= \sum_{x\in K^*} T^i(x^{-1}) \sum_{z\in K} \delta_S(z-x)[z] \\
&= \frac{1}{\ell}\left(\sum_{x\in K^*} T^i(x^{-1}) \sum_{z\in K}\sum_{m=0}^{\ell-1} T^{mk}(z-x)[z] - \sum_{x\in K^*} T^i(x^{-1})[x]\right) \\
&= \frac{1}{\ell}\left(\sum_{x\in K^*} T^i(x^{-1}) \sum_{z\in K}\sum_{m=0}^{\ell-1} T^{mk}(z-x)[z] - f_i\right) \\
&= \frac{1}{\ell}\left(\sum_{x\in K^*} T^i(x^{-1}) \sum_{z\in K^*}\sum_{m=0}^{\ell-1} T^{mk}(z-x)[z] + \sum_{x\in K^*} T^i(x^{-1}) \sum_{m=0}^{\ell-1} T^{mk}(-x)[0] - f_i\right)
\end{aligned}
$$

We have $-1 \in S$, and thus $T^{m\ell}(-x) = T^{m\ell}(x)$.

$$
\begin{aligned}
&= \frac{1}{\ell}\left(\sum_{x\in K^*} T^i(x^{-1}) \sum_{z\in K^*}\sum_{m=0}^{\ell-1} T^{mk}(z-x)[z] + \sum_{m=0}^{\ell-1}\sum_{x\in K^*} T^{i-mk}(x^{-1})[0] - f_i\right) \\
&= \frac{1}{\ell}\left(\sum_{x\in K^*} T^i(x^{-1}) \sum_{z\in K^*}\sum_{m=0}^{\ell-1} T^{mk}(z-x)[z] + \delta(i)(q-1)[0] - f_i\right)
\end{aligned}
$$

(Here δ denotes the characteristic function of $\{m\ell | 0 \leq m \leq k-1\}$.)

$$
\begin{aligned}
&= \frac{1}{\ell}\left(\sum_{m=0}^{\ell-1}\sum_{x\in K^*} T^i(x^{-1}) \sum_{z\in K^*} T^{mk}(z)T^{mk}(1-x/z)[z] + \delta(i)(q-1)[0] - f_i\right) \\
&= \frac{1}{\ell}\left(\sum_{m=0}^{\ell-1}\sum_{z\in K^*}\sum_{x\in K^*} T^i(z^{-1})T^{mk}(z)T^{-i}(x/z)T^{mk}(1-x/z)[z] + \delta(i)(q-1)[0] - f_i\right) \\
&= \frac{1}{\ell}\left(\sum_{m=0}^{\ell-1}\sum_{z\in K^*} T^{i-mk}(z) \sum_{y\in K^*} T^{-i}(y)T^{mk}(1-y)[z] + \delta(i)(q-1)[0] - f_i\right) \\
&= \frac{1}{\ell}\left(\sum_{m=0}^{\ell-1} J(T^{-i}, T^{mk}) f_{i-mk} + \delta(i)(q-1)[0] - f_i\right)
\end{aligned}
$$

From the general theory of Jacobi sums, we have $J(\lambda, \lambda^{-1}) = -\lambda(-1)$. Since $-1 \in S$, we have $T^{m\ell}(-1) = 1$, therefore we have $J(T^{-m\ell}, T^{m\ell}) = -1$. Now (1) and (2) follow from these calculations and results (3) and (4) are straightforward. □

We recall that the eigenvalues of L are 0,u and v, with multiplicities 1, k and $(\ell-1)k$ (same as $q-k-1$), respectively (c.f §3). Again from §3 we know that the nullity of L is 1. Now since the nullity of L_0 is 1 (c.f Lemma 8), all other L_i's are invertible. It follows that for $i \neq 0$, the characteristic polynomial of L_i is a polynomial of the form $(x-u)^a(x-v)^b$ with $a, b \in \mathbb{N}$. By Lemma 8, we have $q = tr(L_i) = au + bv$. It now follows that $a = 1$ and $b = \ell - 1$. By similar arguments, we may show that the eigenvalues of L_0 are 0,u and v with multiplicities 1,1 and $\ell-1$, respectively. We have proved the following Lemma.

Lemma 9. (1) *For $i \neq 0$, the eigenvalues of L_i are u and v with multiplicities* 1 *and* $\ell - 1$, *respectively.*
(2) *The eigenvalues of L_0 are* 0, *u and v with multiplicities* 1 1 *and* $\ell-1$, *respectively.*

7. The Sylow p-subgroup of the critical group of $G(p, \ell, t)$

From the previous section it is clear that the *critical* group C of the graph is

$$\bigoplus_{i=1}^{k-1} \operatorname{coker}(L_i) \bigoplus \operatorname{Tor}(\operatorname{coker}(L_0)).$$

As ℓ is a unit in R, the Smith normal form of L_i is the same as that of ℓL_i. The entries of ℓL_i are either q or a Jacobi sum of the form $J(T^{-(i+mk)}, T^{-nk})$, where $0 \leq m \leq \ell-1$ and $0 < n \leq \ell-1$. By C_i we denote the abelian group $\operatorname{Tor}(\operatorname{coker}(L_i))$.

Lemma 9 implies that for $i \neq 0$ we have $v_p(|C_i|) = v_p(\det(L_i)) = v_p(u) + (\ell - 1)v_p(v)$. By Kirchoff's matrix tree theorem we have $v_p(|C|) = kv_p(u) + (\ell-1)kv_p(v) - v_p(q)$. We can now conclude that $v_p(|C_0|) = v_p(|C|) - \sum_{i\neq 0} v_p(|C_i|) = v_p(u) + (\ell - 3)v_p(v)$.

An integer x not divisible by $q - 1$ has, when reduced modulo $q - 1$, a unique p-digit expansion $x \equiv a_0 + a_1 p + \ldots + a_{(\ell-1)t-1} p^{(\ell-1)t-1} \pmod{q-1}$, where $0 \leq a_i \leq p - 1$. We represent this expansion by the tuple of digits $(a_0, \ldots, a_i, \ldots, a_{(\ell-1)t-1})$. By $s(x)$ we denote the sum $\sum a_i$. For example, 1 has the expansion $(1, \ldots 0 \ldots 0)$ and $s(1) = 1$. Let $p \equiv a \pmod{\ell}$, and for $b \in \mathbb{Z}$ let $[b]$ denote the unique positive integer less than ℓ satisfying $b \equiv [b] \pmod{\ell}$. We can now see that

$$\begin{aligned} k &= \frac{q-1}{\ell} \\ &= \frac{p^{\ell-1}-1}{\ell} \frac{p^{(\ell-1)t}-1}{p^{\ell-1}-1} \\ &= \sum_{r=0}^{\ell-2} \left(\frac{[a^r]p - [a^{r+1}]}{\ell} \right) p^{\ell-2-r} \times \sum_{m=0}^{t-1} p^{(\ell-1)m}. \end{aligned}$$

Thus in the notation we adopted, the tuple for k is the tuple in which the string

$$\left(\frac{[a^{\ell-2}]p - 1}{\ell}, \ldots, \frac{[a^i]p - [a^{i+1}]}{\ell}, \ldots, \frac{p - [a]}{\ell} \right)$$

repeats t times. As p is primitive modulo ℓ, we have $\{[a^i] | 0 \leq i \leq \ell - 2\} = \{1, 2, \ldots \ell - 1\}$. We can now conclude that $s(k) = \frac{(\ell-1)t}{2}$.

Now for $0 \leq i, j \leq \ell - 2$, let $[a^{i+1}][a^j] = [a^{i+j+1}] + rp$. Then we have

$$\begin{aligned} &\frac{[a^j][a^i]p - [a^j][a^{i+1}]}{\ell} p^{\ell-2-i} + \frac{[a^j][a^{i+1}]p - [a^{i+2}][a^j]}{\ell} p^{\ell-2-i-1} \\ = &\frac{[a^j][a^i]p - [a^{i+j+1}] - rp}{\ell} p^{\ell-2-i} + \frac{[a^{i+j+1}]p + rp^2 - [a^{i+2}][a^j]}{\ell} p^{\ell-2-i-1} \\ = &\frac{[a^j][a^i]p - [a^{i+j+1}]}{\ell} p^{\ell-2-i} + \frac{[a^{i+j+1}]p - [a^{i+2}][a^j]}{\ell} p^{\ell-2-i-1}. \end{aligned}$$

This implies that the tuple representing $[a^j]k$ is the tuple in which the string

$$\left(\frac{[a^{\ell+j-2}]p - 1}{\ell}, \ldots, \frac{[a^{i+j}]p - [a^{i+j+1}]}{\ell}, \ldots, \frac{[a^j]p - [a^{j+1}]}{\ell} \right)$$

repeats t times. We may now conclude that for all $1 \leq m \leq \ell - 1$, we have $s(mk) = s(k) = (\ell - 1)t$.

Applying Stickelberger's theorem on Gauss Sums [21] and the well know relation between Gauss and Jacobi sums we can deduce the following theorem.

Theorem 10. *Let q be a power of a prime p and let a and b be integers not divisible by $q - 1$. If $a + b \not\equiv \pmod{q-1}$, 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 $q - 1$.

Given a, b as described in the theorem above, by $c(a, b)$ we denote $v_p(J(T^{-a}, T^{-b}))$. Then by Lemma 8 the off-diagonal entries of L_i (with $i \neq 0$) are $u_{mn} p^{c(i+mk,nk)}$ for some units u_{mn} of R, and the diagonal entries are all q/ℓ. As discussed in the beginning of this section we have $v_p(|C_i|) = v_p(u) + (\ell - 1)v_p(v)$. By some abuse of notation, we denote f_i to be the column vector representing f_i with respect to the standard basis on R^K. Then we have $J(f_i) = \left(\sum_{x \in K^*} T^{-i}(x) \right) \mathbf{1}$, where $\mathbf{1}$ is the all-one vector. Thus for $i \neq 0$, since T^{-i} is a non-trivial character, we have $J(f_i) = 0$ for $i \neq 0$. Using this and 3.1, we can now conclude that L_i satisfies $(x - u)(x - v) = 0$. We make use of this to arrive at the following lemma.

Lemma 11. *Given $j < \frac{(\ell-1)t}{2}$ and $0 < i \leq k - 1$, the multiplicity of p^j as an elementary divisor of C_i is the same as that of $p^{v_p(uv)-j}$.*

Proof. As L_i satisfies $(x-u)(x-v)=0$, we have $(L_i)(L_i-(v+u)I)=vuI$. Let P and Q be unimodular matrices such that PLQ is the Smith normal form of L. Now consider $PL_iQQ^{-1}(L_i-(v+u)I)P^{-1}=vuI$. This shows that the multiplicity of p^j as an elementary divisor of L_i is the same as the multiplicity of $p^{v_p(uv)-j}$ as an elementary divisor of $L_i-(v+u)I$. Since L_i and $L_i-(u+v)I$ are congruent modulo $p^{v_p(v)}=p^{(\ell-1)t/2}$, for $0\le j<(\ell-1)t/2$ the multiplicity of p^j as an elementary divisor of L_i is the same as the multiplicity of p^j as an elementary divisor of $L_i-(v+u)I$. $\square$

Following the notation in §5, we consider the vector spaces $\overline{M}_y(L_i)$. We have $v_p(C_i)=v_p(u)+(\ell-1)v_p(v)$. Let $c=\min(\{c(i+mk,nk)|0\le m\le\ell-1 \text{ and } 0\le n\le\ell-1\})$. By Theorem 10, we have $c(i+mk,nk)+c(i+(m+n)k,(\ell-n)k)=(\ell-1)t$. We can now conclude that $c\le\ell(\ell-1)t/2$. Let $\operatorname{diag}(\beta_1,\beta_2,\dots\beta_\ell)$ be the Smith normal form of L_i. Then by Lemma 8 and Lemma 4, it follows that $c=v_p(\beta_1)$. By definition of $M_c(L_i)$ it follows that $M_c(L_i)=N_i$ and thus $\dim(\overline{M}_c(L_i)=\ell$. Assume $c<(\ell-1)t/2$, then by Lemma 11 we have $e_{v_p(uv)-c}(L_i)=e_c(L_i)\ge1$ and thus $\dim(\overline{M_{v_p(uv)-c}}(L_i))\ge1$. Lemma 9 tell us that multiplicity of v as an eigenvalue of L_i is $\ell-1$. Now Lemma 7 implies that $\dim(\overline{M}_{(\ell-1)t/2})\ge\ell-1$. As $\dim(\overline{M}_c(L_i)-dim(\overline{M}_{(\ell-1)t/2}(L_i))\ge1$ we have $\dim(\overline{M}_c(L_i))\ge\ell$. Therefore by Lemma 6, setting $z=3$, $s_1=\ell, s_2=\ell-1, s_3=1, s_4=\overline{Ker(L_i)}=0$, $t_1=c, t_2=(\ell-1)t/2$, and $t_3=v_p(uv)-c$, we have $e_c(L_i)=e_{v_p(uv)-c}(L_i)=1$, $e_{(\ell-1)t/2}(L_i)=\ell-2$, and $e_i(L_i)=0$ for all other i. Now assume that $c=(\ell-1)t/2$. Lemma 7 implies that $dim(\overline{M}_{v_p(u)}(L_i))\ge1$, since u is an eigenvalue of multiplicity 1. Therefore by Lemma 6, setting $z=2$, $s_1=\ell$, $s_2=1$, $s_3=\overline{Ker(L_i)}$, $t_1=(\ell-1)t/2$, and $t_2=v_2(v)$, we have $e_c(L_i)=\ell-1$, $e_{v_p(v)}(L_i)=1$, and $e_i(L_i)=0$ for all other i. Thus the Smith normal form of L_i over R_p is the diagonal matrix $\operatorname{diag}(p^c,\underbrace{p^{(\ell-1)t/2},\dots,p^{(\ell-1)t/2}}_{(\ell-2)\text{ repetitions}},p^{v_p(uv)-c})$.

In the beginning of the section, we showed that $v_p(|C_0|)=v_p(u)+(\ell-3)v_p(v)$. By Lemma 8 and Theorem 10, there are units $v_{(mn)}$ in R_p such that the matrix ℓL_0 is

$$\begin{bmatrix} q & v_{(12)}\sqrt{q} & \dots & v_{(1\ \ell-1)}\sqrt{q} & -1 & 0\\ \vdots & \ddots & \dots & \vdots & \vdots & \vdots\\ v_{(\ell-1\ 1)}\sqrt{q} & \dots & \dots & q & -1 & 0\\ -q & \dots & \dots & -q & q & 0\\ 1 & \dots & \dots & 1 & -1 & 0 \end{bmatrix}.$$

The determinant of the 2×2 minor $\begin{bmatrix} q & -1\\ 1 & -1\end{bmatrix}$ of ℓL_0 is a unit in R_p. Observe that any 3×3 minor of ℓL_0 has p-valuation of atleast $v_p(q)$. Now applying Lemma 4 yields that the multiplicity of $p^0=1$ as an elementary divisor of L_0 is 2. Following the notation in §5, we have $e_0(L_0)=2$. Now Lemma 5 implies that $\dim(\overline{M}_0(L_0))-\dim(\overline{M}_1(L_0))=2$, and thus we have $\dim(\overline{M}_1(L_0))=\ell+1-2=\ell-1$. By Lemma 9 and Lemma 7, we have $\dim(M_{v_p(v)}(L_0))\ge\ell-1$. Since $\overline{M}_1(L_0)\supset\overline{M}_{v_p(v)}(L_0)$, we have $\dim(\overline{M}_{v_p(v)}(L_0))=\ell-1$. Lemma 8 implies that $\overline{Im(L)}$ is generated by $\mathbf{1}$ and $\sum_{j\neq0}f_{jk}+\mathbf{1}$. Therefore $\dim(\overline{Im(L_0)})=2$. As $LJ=0$, by 3.1 the restriction of L to $Im(L)$ satisfies $L(L-t+uI)=tuI$. As $Im(L_0)\subset Im(L)$, we can conclude that $\overline{Im(L_0)}\subset\overline{M}_{v_p(uv)}(L_0)\subset\overline{M}_{v_p(u)}(L_0)$.

We have $v_p(|C_0|)=v_p(v)(\ell-1-2)+v_p(u)(2-1)$. Therefore by applying Lemma 6, we can conclude that the Smith normal form of L_0 over R_p is $\operatorname{diag}(1,1,\underbrace{p^{(\ell-1)t/2}}_{\ell-3\text{ times}},p^{v_p(u)},0)$.

7.1. **Proof of Theorem 1.** As observed in §6, the Laplacian matrix L is similar over R_p to the block diagonal matrix $\operatorname{diag}(L_0,L_1,L_2\dots L_{k-1})$. From the discussion above, the Smith normal form of L_i over R_p is

$\operatorname{diag}(p^{c_i},\underbrace{p^{(\ell-1)t/2},\dots,p^{(\ell-1)t/2}}_{(\ell-2)\text{ repetitions}},p^{v_p(uv)-c})$

and that of L_0 is $\operatorname{diag}(1,1,\underbrace{p^{(\ell-1)t/2}}_{\ell-3\text{ times}},p^{v_p(u)},0)$. Results (1) − (3) are now immediate.

If $p\nmid\ell-1$, we have $v_p(u)=\frac{(\ell-1)t}{2}=v_p(v)=v_p(uv)-\frac{(\ell-1)t}{2}$. Applying $q-1=\sum e_j$ along with (1) and (3) yields (4). If $p\mid\ell-1$, then $v_p(u)>\frac{(\ell-1)t}{2}t=v_p(v)$ and $v_p(u)=v_p(uv)-\frac{(\ell-1)t}{2}$. If $1\le i\le k-1$ is such that $c_i=\frac{(\ell-1)t}{2}t$, then the Smith normal form of L_i has $\ell-1$ repetitions of $p^{\frac{(\ell-1)t}{2}t}$ and one $p^{v_p(u)}$. The Smith normal form of L_0 is

$diag(1,1,\underbrace{p^{(\ell-1)t/2}}_{\ell-3 \text{ times}},p^{v_p(u)},0)$. We can now see that $e_{v_p(u)}-1+(\ell-2)(k-1)+(\ell-3)=e_{\frac{(\ell-1)t}{2}}$. The previous equality and $q-1=e_{v_p(u)}+e_{\frac{(\ell-1)t}{2}}-2+2\sum_{j<t}e_j$ yield (5).

(6) follows from the Smith normal form's of L_i's.

8. The Critical group of $G(p,3,t)$

We now turn our focus to graphs of the form $G(p,3,t)$. We assume that $(p,t)\neq(2,1)$ and $p\equiv 2 \pmod 3$, so these graphs are connected and strongly regular. Recall that this is the Cayley graph on the additive group of the field $K=\mathbb{F}_q$ ($q=p^{2t}$) with "connection set" S, where S is the unique subgroup of K^* satisfying $k:=|S|=\frac{q-1}{3}$. All the results in the previous sections transfer to this case by setting $\ell=3$.

We have shown in the previous section that for $i\neq 0$, the Smith normal form of L_i over R_p is $\mathrm{diag}(p^c,p^t,p^{v_p(uv)-c})$. Here c is the least among the $p-$valuations of the entries of L_i. Here $v=\sqrt{q}\dfrac{\sqrt{q}+(-1)^{t+1}}{3}$, and $u=v+(-1)^t\sqrt{q}$ are the non-zero eigenvalues of the Laplacian of $G(p,3,t)$.

Given integers a,b not divisible by $q-1$, let $c(a,b)$ denote the number of carries when adding the p-adic expansions of a and $b \pmod{q-1}$. Consider the following counting problem.

Counting Problem: For $1\leq i\leq k-1$, by $c(i)$ we denote $\min(\{c(i+mk,nk)|\ 0\leq m\leq 2, \text{ and } n=1,2\})$. Given $0\leq a<t$, find $|\{i|\ c(i)=a\}|$.

Given a positive integer b, by e_a we denote the multiplicity of p^a as an elementary divisor of the *critical* group of $G(p,3,t)$. Let e_0 be the p-rank of the Laplacian of $G(p,3,t)$. Theorem 1 implies that, for $0<a<t$, we have $e_a=|\{i|\ c(i)=a\}|$, and $e_0=|\{i|\ c(i)=0\}|+2$. Thus the solution to this problem will immediately provide us with the elementary divisor form of the *critical* groups of graphs of the form $G(p,3,t)$.

For $0\leq a<q-1$, let a_m denote the mth digit in the p-adic expansion of a, i.e $a=\sum_{m=0}^{2t-1}a_mp^m$. By $s(a)$, we denote $\sum a_m$. We may observe from Theorem 10 that

$$c(a,b)=\frac{s(a)+s(b)-s(a+b)}{p-1}. \tag{8.1}$$

The even digits (in the p-adic expansion) of k are $\frac{p-2}{3}$ and the odd digits are $\frac{2p-1}{3}$. The digits of $2k$ are the same as that of k, but with opposite parity. Thus we have $s(k)=s(2k)=t$. Given $j\in\mathbb{Z}$, by $\overline{j}$ we denote the unique element of $\{0,1,\ldots,q-2\}$ satisfying $j\equiv\overline{j} \pmod{q-1}$.

The following follows from 8.1.

Lemma 12. *Given $j\in\{0,1,\ldots,q-2\}$ and $m=0,1,2$, the following hold.*

1. $c(j,\overline{mk})+c(\overline{j+mk},\overline{-mk})=2t$
2. $c(j,\overline{-mk})+c(\overline{j-mk},\overline{mk})=2t$
3. $c(\overline{j-mk},\overline{-mk})+c(j,\overline{-mk})=t+c(j,\overline{mk})$
4. $c(j,mk)+c(\overline{j+mk},mk)=t+c(j,\overline{-mk})$
5. $c(j,mk)=c(\overline{-j-mk},mk)$
6. $c(\overline{-j-mk},\overline{-mk})=c(\overline{j-mk},\overline{-mk})$

Let $j\in\{1,\ldots,q-2\}\setminus\{k,2k\}$, define $g(j):=\{c(j,k),c(j,2k)\}$. For every j, there is a unique $\phi(j)\in\{1,2\ldots,k-1\}$ such that $j-\phi(j)\in\{0,k,2k\}$. Note that $\phi^{-1}(i)=\{i,i+k,i+2k\}$.

Define $Y_a:=\{j\mid g(j)=\{a,b\}$ for some b such that $a\leq b\leq t\}$ and $R_a=\{i|1\leq i\leq k-1$ and $c(i)=a\}$.

Lemma 13. *Given Y_a and ϕ defined above and $a<t$, the following are true.*

1. *If ϕ_a is the restriction of ϕ to Y_a, then $\phi_a(Y_a)=R_a$.*
2. *Let $i\in R_a$ and $j\in\{i,i+k,i+2k\}\cap\phi_a^{-1}(i)$ with $c(j,mk)=a$ for some $m\in 1,2$. Then*
   (a) *$\{i,i+k,i+2k\}\cap\phi_a^{-1}(i)=\{j\}$ if and only if $a\leq c(j,-mk)<t$;*
   (b) *and $\{i,i+k,i+2k\}\cap\phi_a^{-1}(i)=\{j,\overline{j-mk}\}$ if and only if $c(j,\overline{-mk})=t$.*
3. *For $0\leq a<t$, we have $e_a=|R_a|=|Y_a|-1/2|\{j|\ g(j)=\{a,t\}\}|=|Y_a|-|\{j|\ g(j)=\{a\}\}|$*

Proof. 1) Let $m\in 1,2$ and $j\in Y_a$ such that $c(j,mk)=a$, and $c(j,\overline{-mk})=b$. Then by Lemma 12, we have $\{c(\overline{j+mk},nk)|\ 0\leq m\leq 2, \text{ and } n=1,2\}=\{a,b,t-a+b,t-b-a,2t-a,2t-b\}$. Since $a\leq b\leq t$, we have $c(\phi(j))=a$.

thus $\phi_a(Y_a) \subset R_a$. If $i \in R_a$, then there exists $j \in \{i, i+k, i+2k\}$ and $m \in \overline{1,2}$ such that $c(j, mk) = a$. Since $a = \min(\{c(i+mk, nk) | 0 \le m \le 2, \text{ and } n = 1, 2\})$, we have from 8.1 $c(j, mk) \le c(\overline{j - mk}, \overline{-mk}) = t + c(j, mk) - c(j, \overline{-mk})$. Thus we have $c(j, \overline{-mk}) \le t$ and therefore $j \in Y_a$ and $\phi_a(j) = i$.

2) If $c(j, mk) = a$, then since $c(j, mk) + c(\overline{j+mk}, \overline{-mk}) = 2t$ and $c(j, mk) + c(\overline{j+mk}, mk) = t + c(j, \overline{-mk})$ and $c(j, \overline{-mk}) \ge c(j, mk)$ (as $j \in Y_a$), we have $j + mk \notin \phi_a^{-1}(i)$. Thus we have $\phi_a^{-1}(i) \subset \{j, \overline{j - mk}\}$

As $j \in Y_a$, we have that $c(j, \overline{-mk}) \le t$ and thus $c(\overline{j - mk}, mk) = 2t - c(j, mk) \ge t$. We have $c(\overline{j - mk}, \overline{-mk}) + c(j, \overline{-mk}) = t + c(j, mk)$, and thus $c(\overline{j - mk}, \overline{-mk}) = a$ if and only if $c(j, \overline{-mk}) = t$. Thus $\overline{j - mk} \in Y_a$ is and only if $c(j, \overline{-mk}) = t$. Thus 2 is true.

3) From the proof of 2), we have $g(j) = \{a, t\}$ if and only if $g(\overline{j - mk}) = \{t, a\}$. Thus we have $|R_a| = |Y_a| - |\{j | g(j) = \{a, t\}\}|$. Using Lemma 1 and $s(l) + s(-l) = 2t(p-1)$ we can deduce that $c(j, mk) = c(\overline{-j - mk}, mk)$ and $c(\overline{-j - mk}, \overline{-mk}) = c(\overline{j - mk}, \overline{-mk})$. Thus the map $\lambda : \{j | g(j) = \{a, t\}\} \to \{j | g(j) = \{a\}\}$ defined by $\lambda(j) = \overline{-j - k}$ is a 2 to 1 map.

□

Corollary 14. $e_0 = \left(\dfrac{p+1}{3}\right)^{2t} (2^{t+1} - 2)$.

Proof. By the above Lemma, we have $e_0 = |Y_0| - \{j | g(j) = \{0\}\} + 2$. The set $\{j | (c(j, k), c(j, 2k)) = (0, b)\}$ consists of $j \ne 0, 2k$ whose even digits are between 0 and $\frac{p+1}{3}$ and the odd digits lie between 0 and $\frac{2(p+1)}{3}$. Thus this set has size $2^t \left(\dfrac{p+1}{3}\right)^{2t} - 2$. Similarly $|\{j | j \ne 0 \text{ and } (c(j, k), c(j, 2k)) = (b, 0)\}| = 2^t \left(\dfrac{p+1}{3}\right)^{2t} - 2$. Similar computations yield $|\{j | j \ne 0 \text{and} g(j) = \{0\}\}| = \left(\frac{p+1}{3}\right)^{2t} - 1$. The result now follows by the principle of inclusion-exclusion. □

We will use the transfer matrix method to compute e_a.

Consider $A = \{(\alpha, \gamma, \delta) | (\alpha, \gamma, \delta) \in [p] \times [2] \times [2]\}$ and $B = \{[\alpha, \gamma, \delta] | (\alpha, \gamma, \delta) \in [p] \times [2] \times [2]\}$. We construct a bipartite digraph $D = (A, B, E)$. There is an arc e $\in E$ from $(\alpha, \gamma, \delta) \in A$ to $[\alpha', \gamma', \delta'] \in B$ if an only if

$$\alpha + \frac{2p-1}{3} + \gamma = \beta + p\gamma'$$

and

$$\alpha + \frac{p-2}{3} + \delta = \epsilon + p\delta'$$

for some $\beta, \epsilon \in [p]$. There is an arc $\mathrm{e}_\lambda \in E$ from $[\alpha, \gamma, \delta] \in B$ to $(\alpha', \gamma', \delta') \in A$ if and only if

$$\alpha + \frac{p-2}{3} + \gamma = \beta + p\gamma'$$

and

$$\alpha + \frac{2p-1}{3} + \delta = \epsilon + p\delta'$$

for some $\beta, \epsilon \in [p]$. The arcs in D of type e and e_λ are assigned label α and weights $wt(\mathrm{e}) = wt(\mathrm{e}_\lambda) = x^{\gamma'} y^{\delta'}$. So we have a weight function $wt : E \to \mathbb{C}[x, y]$ on D. The weight of a walk on D will be the products of the weights of its arcs.

Given $a, b \in [2t+1]$, define E_{ab} to be the set of closed of length $2t$ and weight $x^a y^b$. A closed walk of length $2t$ with its initial vertex in A is said to be of type A, and it is of Type B otherwise. Let $Y_{ab} = \{j \in [q-1] | g(j) = \{a, b\}\}$. Let $a_0, a_1, \ldots a_{2t}$ be the labels of arcs of a walk $w \in \cup E_{ab}$, then define $\psi(w) = \sum a_i p^i$. When $\{a, b\} \ne \{0\}$ and $\ne \{2t\}$, we have $\psi(E_{ab}) \subset Y_{ab}$. By the p-ary add-with-carry-algorithm described in Theorem 4.1 of [13], given $j \in Y_{ab}$, there exist *carry sequences* $(\gamma_0, \gamma_1, \ldots \gamma_{2t-1})$ and $(\delta_0, \delta_1, \ldots \delta_{2t-1})$ with $\gamma_i, \delta_i \in [2]$ such that

$$a_i + \frac{2p-1}{3} + \gamma_i = b_i + \gamma_{i+1} p \qquad a_i + \frac{p-2}{3} + \delta_i = d_i + \delta_{i+1} p\ , \text{ for even } i \text{ and;}$$

$$a_i + \frac{p-2}{3} + \gamma_i = b_i + \gamma_{i+1} p \qquad a_i + \frac{2p-1}{3} + \delta_i = d_i + \delta_{i+1} p\ , \text{ for odd } i;$$

here $j = \sum a_i p^i$, $j + k = \sum b_i p^i$ and $j + 2k = d_i p^i$. We can now see that there are exactly two closed walks, one of each type which map to j under ψ. If $w(j, A)$ (resp. $w(j, B)$) is the walk of type A such that $\psi(w(A, j)) = j$ (resp.

$\psi(w(A, j)) = j$), then $wt(w(A, j)) = x^{c(j,k)}y^{c(j,2k)}$ (resp. $wt(w(A, j)) = x^{c(j,2k)}y^{c(j,k)}$). Thus we concluded that for $a \neq b$, the restriction of ψ is a bijection from E_{ab} to Y_{ab}. Applying Lemma 13 3) gives us

$$e_a = \sum_{b=a+1}^{t} |E_{ab}|, \tag{8.2}$$

for all $0 < a < t$.

We observe that for all $\alpha, \alpha' \in [p]$ and $\gamma, \delta \in [2] \times [2]$, there is no arc from (α, γ, δ) (resp. $[\alpha, \gamma, \delta]$) to $[\alpha', 0, 1]$ (resp. $(\alpha', 1, 0)$). We may also conclude that

(1) (α, γ, δ) is adjacent to $[\alpha', 0, 0]$ if and only if $0 \leq \alpha < \frac{p+1}{3} - \gamma$;
(2) (α, γ, δ) is adjacent to $[\alpha', 1, 0]$ if and only if $\frac{p+1}{3} - \gamma \leq \alpha < \frac{2(p+1)}{3} - \delta$;
(3) (α, γ, δ) is adjacent to $[\alpha', 1, 1]$ if and only if $\frac{2(p+1)}{3} - \delta \leq \alpha < p$;
(4) $[\alpha, \gamma, \delta]$ is adjacent to $(\alpha', 0, 0)$ if and only if $0 \leq \alpha < \frac{p+1}{3} - \delta$;
(5) $[\alpha, \gamma, \delta]$ is adjacent to $(\alpha', 0, 1)$ if and only if $\frac{p+1}{3} - \delta \leq \alpha < \frac{2(p+1)}{3} - \gamma$;
(6) and $[\alpha, \gamma, \delta]$ is adjacent to $(\alpha', 1, 1)$ if and only if $\frac{2(p+1)}{3} - \gamma \leq \alpha < p$.

Let M be the adjacency matrix of the weighted digraph D and let U be the $\mathbb{C}(x, y)$ vector space generated by the vertex set $A \cup B$ (of D) as a basis. By abuse of notation, we may assume $M \in \mathrm{End}(U)$.

Let $h_1 := \sum_{(\gamma,\delta)} \sum_{\alpha' < \frac{p+1}{3} - \gamma} [\alpha', \lambda, \delta]$, $h_2 = \sum_{(\gamma,\delta)} \sum_{\frac{p+1}{3} - \gamma \leq \alpha' < \frac{2(p+1)}{3} - \delta} [\alpha', \lambda, \delta]$, $h_3 = \sum_{(\gamma,\delta)} \sum_{\alpha' \geq \frac{2(p+1)}{3} - \delta} [\alpha', \lambda, \delta]$. We define f_1, f_2, and f_3 by exchanging the roles of γ and δ and replacing $[\alpha', \gamma, \delta]$ with $(\alpha', \gamma, \delta)$. We can see that $M(A \cup B) = \{h_1, h_2, h_3, f_1, f_2, f_3\}$. We also have.

$$\begin{aligned}
M(f_1) &= \frac{p+1}{3}h_1 + \frac{p+1}{3}xh_2 + \frac{p-2}{3}xyh_3,\\
M(f_2) &= \frac{p+1}{3}h_1 + \frac{p-2}{3}xh_2 + \frac{p+1}{3}xyh_3,\\
M(f_3) &= \frac{p-2}{3}h_1 + \frac{p+1}{3}xh_2 + \frac{p+1}{3}xyh_3,\\
M(h_1) &= \frac{p+1}{3}f_1 + \frac{p+1}{3}yf_2 + \frac{p-2}{3}xyf_3,\\
M(h_2) &= \frac{p+1}{3}f_1 + \frac{p-2}{3}yf_2 + \frac{p+1}{3}xyf_3, \text{ and}\\
M(h_3) &= \frac{p-2}{3}f_1 + \frac{p+1}{3}yf_2 + \frac{p+1}{3}xyf_3.
\end{aligned}$$

Let W be the subspace of U generated by $\{h_1, h_2, h_3, f_1, f_2, f_3\}$. We have $M(U) = W$. The set $\beta = \{h_1, h_2, h_3, f_1, f_2, f_3\}$ is linearly independent, and thus a basis for W. Let $M_{[\beta]}$ be the matrix of $M|_W$ with respect to the basis β of W. From above we see that $M_{[\beta]}$ is

$$\begin{bmatrix}
0 & 0 & 0 & \frac{p+1}{3} & \frac{p+1}{3} & \frac{p-2}{3}\\
0 & 0 & 0 & \frac{p+1}{3}y & \frac{p-2}{3}y & \frac{p+1}{3}y\\
0 & 0 & 0 & \frac{p-2}{y}xy & \frac{p+1}{3}xy & \frac{p+1}{3}xy\\
\frac{p+1}{3} & \frac{p+1}{3} & \frac{p-2}{3} & 0 & 0 & 0\\
\frac{p+1}{3}x & \frac{p-2}{3}x & \frac{p+1}{3}x & 0 & 0 & 0\\
\frac{p-2}{y}xy & \frac{p+1}{3}xy & \frac{p+1}{3}xy & 0 & 0 & 0
\end{bmatrix}.$$

As $det(M_\beta) = -p^2x^3y^3 \neq 0$, we have $W \cap \ker(M) = \{0\}$ and thus $U = \ker(\mathrm{M}) \oplus W$.

Thus the characteristic polynomial of M is $f(z) = z^{8p-6}\det(zI - M_{[\beta]})$. Using a computer algebra software such as Sage, we may conclude that $det(zI - M_\beta) = z^6 - Pz^4 + Qz^2 - R$,

where $P = \left(\left(\frac{p+1}{3}\right)^2 (x^2y^2 + x^2y + xy^2 + x + y + 1) + \left(\frac{p-2}{3}\right)^2 3xy\right)$,

$Q = \left(\left(\frac{p+1}{3}\right)^2 (xy)(x^2y^2 + x^2y + xy^2 + x + y + 1) + \left(\frac{2p-1}{3}\right)^2 3x^2y^2\right)$, and $R = p^2x^3y^3$. Thus $f(z) = z^{8p} - Pz^{8p-2} + Qz^{8p-4} - Rz^{8p-6}$.

Let $C(n) = \sum_{\psi} wt(\psi)$, where the sum is over closed walks in D of length n. As D is a bipartite graph $C(n) = 0$ for all odd n. By Corollary 4.7.3 of [19], we have

$$\sum_{t \geq 1} C(2t) z^{2t} = -\frac{zT'(z)}{T(z)},$$

where $T(z) = det(I - zM)$. The characteristic polynomial of M was computed above to be $z^{8p} - Pz^{8p-2} + Qz^{8p-4} - Rz^{8p-6}$, and thus we have

$$\sum_{t \geq 1} C(2t) z^{2t} = \frac{2Pz^2 - 4Qz^4 + 6Rz^6}{1 - (Pz^2 - Qz^4 + Rz^6)}.$$

Let $C(2t) = 0$ for $t \leq 0$. We have $\sum_{t \geq 1} (C(2t) - PC(2t-2) + QC(2t-4) - RC(2t-6)) z^t = 2Pz - 4Qz^2 + 6Rz^3$. Thus we have

$$\begin{aligned} C(2) &= 2P \\ C(4) &= 2(P^2 - 2Q), \\ C(6) &= 6R + 2(P^3 - 2QP) - 2PQ, \\ \text{and } C(2t) &= PC(2t-2) - QC(2t-4) + RC(2t-6) \text{ for } t > 3. \end{aligned}$$

The coefficient of $x^a y^b$ in $C(2t)$ is E_{ab}. Given $a < t$, we have from 8.2 that $e_a = \sum_{a < b \leq t} E_{ab}$. Application of Theorem 1 and Corollary 14 yield Theorem 2.

Acknowledgement

I thank Prof. Peter Sin for his valuable suggestions and feedback. I am grateful to Prof. David Saunders for providing computational data.

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] N.L. Biggs. Chip-firing and the critical group of a graph. *Journal of Algebraic Combinatorics*, 9(1):25–45, Jan 1999.
[5] AE Brouwer, RM Wilson, and Qing Xiang. Cyclotomy and strongly regular graphs. *Journal of Algebraic Combinatorics*, 10(1):25–28, 1999.
[6] 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.
[7] Andries E. Brouwer and Willem H. Haemers. *Spectra of graphs*. Universitext. Springer, New York, 2012.
[8] 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.
[9] Deepak Dhar. Self-organized critical state of sandpile automaton models. *Physical Review Letters*, 64(14):1613, 1990.
[10] 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.
[11] Joshua E Ducey and Peter Sin. The smith group and the critical group of the grassmann graph of lines in finite projective space and of its complement. *arXiv preprint arXiv:1706.01294*, 2017.
[12] Tao Feng, Koji Momihara, and Qing Xiang. Constructions of strongly regular cayley graphs and skew hadamard difference sets from cyclotomic classes. *Combinatorica*, 35(4):413–434, 2015.
[13] 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.
[14] 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.
[15] Dino Lorenzini. Smith normal form and laplacians. *Journal of Combinatorial Theory, Series B*, 98(6):1271 – 1300, 2008.
[16] Venkata Raghu Tej Pantangi and Peter Sin. Smith and critical groups of polar graphs. *arXiv preprint arXiv:1706.08175*, 2017.
[17] Bernhard Schmidt and Clinton White. All two-weight irreducible cyclic codes? *Finite Fields and Their Applications*, 8(1):1–17, 2002.
[18] Peter Sin. The critical groups of the peisert graphs $P^*(q)$. *arXiv preprint arXiv:1606.00870*, 2016.
[19] Richard P. Stanley. *Enumerative Combinatorics: Volume 1*. Cambridge University Press, New York, NY, USA, 2nd edition, 2011.
[20] Richard P Stanley. Smith normal form in combinatorics. *Journal of Combinatorial Theory, Series A*, 144:476–495, 2016.
[21] L. Stickelberger. Ueber eine verallgemeinerung der kreistheilung. *Mathematische Annalen*, 37(3):321–367, Sep 1890.

[22] Jacobus H van Lint and Alexander Schrijver. Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields. *Combinatorica*, 1(1):63–73, 1981.
[23] A. Vince. Elementary divisors of graphs and matroids. *European Journal of Combinatorics*, 12(5):445 – 453, 1991.
[24] Qing Xiang. Cyclotomy, gauss sums, difference sets and strongly regular cayley graphs. In Tor Helleseth and Jonathan Jedwab, editors, *Sequences and Their Applications – SETA 2012*, pages 245–256, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

Email address: pvrt1990@ufl.edu

Department of Mathematics, University of Florida, Gainesville, FL 32611-8105, USA.