The Smith and critical groups of Paley graphs

David B. Chandler · **Peter Sin** · **Qing Xiang**

Abstract There is a Paley graph for each prime power q such that $q \equiv 1 \pmod 4$. The vertex set is the field $\mathbb{F}_q$, and two vertices x and y are joined by an edge if and only if $x - y$ is a nonzero square of $\mathbb{F}_q$. We compute the Smith normal forms of the adjacency matrix and Laplacian matrix of a Paley graph.

Keywords Critical group · Sandpile group · Chip-firing game · Strongly regular graph · Paley graph · Smith normal form · Jacobi sums · Laplacian matrix

1 Introduction

Let Γ be a finite, simple, undirected, and connected graph, and let A be the adjacency matrix of Γ with respect to some fixed but arbitrary ordering of the vertex set of Γ. Let D be the diagonal matrix whose (i, i)-entry is the degree of the ith vertex. Then $L = D - A$ is called the *Laplacian matrix* of Γ. The matrices A and L represent endomorphisms (which will also be denoted by A and L) of the free abelian group on the vertex set. The structure of their cokernels as abelian groups is independent of the above ordering. The cokernel of A is called the *Smith group* $S(\Gamma)$, since its computation is equivalent to finding the Smith normal form of the matrix A. The endomorphism L maps the sum of all vertices to zero; so the cokernel of L is not a

D. B. Chandler
6 Georgian Circle, Newark, DE 19711, USA

P. Sin (✉)
Department of Mathematics, University of Florida, P. O. Box 118105,
Gainesville, FL 32611, USA
e-mail: sin@ufl.edu

Q. Xiang
Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA

torsion group. The torsion subgroup $K(\Gamma)$ of the cokernel of L is called the *critical group* of Γ. It is known, by Kirchhoff's matrix-tree theorem, that the order of $K(\Gamma)$ is equal to the number of spanning trees of Γ.

The critical group of a graph arises in several contexts, for example, in arithmetic geometry [10], in statistical physics [6], and in combinatorics [2]. There are also interpretations of the critical group in discrete dynamics (chip-firing games and abelian sandpile models, cf. [9]). We refer the reader to [11] for a discussion of these and other connections.

So far, there are very few families of graphs for which the critical groups have been found; so it is of some interest to compute the Smith and critical groups for some well-known families of graphs.

In this note, we treat the Paley graphs. Let $q = p^t$ be a fixed prime power with $q \equiv 1 \pmod 4$. The Paley graph Paley(q) is defined by taking the field $\mathbb{F}_q$ as vertex set, with two vertices x and y joined by an edge if and only if $x - y$ is a nonzero square in $\mathbb{F}_q$. The degree of each vertex is $k = \frac{q-1}{2}$. Let A denote the adjacency matrix and $L = kI - A$ the Laplacian matrix. Our main result is the computation of $S(\text{Paley}(q))$ and $K(\text{Paley}(q))$. There has been some earlier work in this direction. The structure of the $S(\text{Paley}(q))$ was correctly conjectured in [13, Ex. 4–8]. In [11], the critical group of a conference graph on a square-free number of vertices was calculated, and Paley(q) is such a graph, when q is a prime. The p-rank of the Laplacian of Paley(q) was first computed in [4].

Here is a brief outline of our method. We view Paley(q) as a Cayley graph, with the regular action of the additive group of $\mathbb{F}_q$. Then, in §2, we follow a standard method, applying the discrete Fourier transform while keeping track of coefficient rings, to compute the Smith group and also the p-complementary part of the critical group. A different approach is needed to compute the p-part of $K(\text{Paley}(q))$. In §3, we study the permutation action of the group S of nonzero squares on $\mathbb{F}_q$ by multiplication and on the free R-module $R^{\mathbb{F}_q}$ with basis $\mathbb{F}_q$ over a suitable extension ring R. The *isotypic component* of an R-free RS-module M with respect to a character $\chi : S \to R^\times$ is defined to be the submodule $\{m \in M \mid sm = \chi(s)m \text{ for all } s \in S\}$. The RS-module $R^{\mathbb{F}_q}$ decomposes into isotypic components of R-rank 2 (except for one of R-rank 3). Since S preserves adjacency, these isotypic components are A-invariant. In the computation of the restriction of A to each isotypic component, certain Jacobi sums arise naturally, and the main problem is reduced to determining the p-adic valuations of these Jacobi sums. The classical theorem of Stickelberger on Gauss sums gives the valuation for individual sums, but there remains the problem of counting the number of sums with a given valuation. This counting problem is solved by the transfer matrix method in §4. It is also possible to count directly, but the chosen method has the advantages of being systematic and of yielding immediately the rationality of the generating function.

2 Eigenvalues and p'-torsion

It is well known and easily checked that Paley(q) is a strongly regular graph and that its eigenvalues are $k = \frac{q-1}{2}$, $r = \frac{-1+\sqrt{q}}{2}$ and $s = \frac{-1-\sqrt{q}}{2}$, with multiplicities 1, $\frac{q-1}{2}$ and $\frac{q-1}{2}$, respectively. (See, for example, [3, §8.1.1]). Hence,

$$|S(\mathrm{Paley}(q))| = \det(A) = k\left(\frac{k}{2}\right)^k,$$

where A is the adjacency matrix of Paley(q). It follows that $\gcd(|S(\mathrm{Paley}(q))|, q) = 1$. Therefore, we can use the diagonalization of A by the character table of $(\mathbb{F}_q, +)$ to find the Smith normal form of A.

Let S be the set of nonzero squares in $\mathbb{F}_q$. We can view Paley(q) as a Cayley graph with connecting set S. Let X be the complex character table of the additive group of $\mathbb{F}_q$, where the elements are ordered in the same way as for the rows and columns of A. The entries of X lie in the ring $\mathbb{Z}[\zeta]$, where ζ is a complex primitive p-th root of unity. As was first observed in [12], we have the character orthogonality relation $\frac{1}{q}X\overline{X}^t = I$ and

$$\frac{1}{q}XA\overline{X}^t = \mathrm{diag}(\psi(S))_\psi, \tag{1}$$

where ψ runs over the additive characters of $\mathbb{F}_q$ and $\psi(S) = \sum_{y \in S}\psi(y)$. Thus, the $\psi(S)$ are the eigenvalues of A. Since the eigenvalues of A are all prime to p, the structure of $S(\mathrm{Paley}(q))$ can be completely determined from (1). (See [14, §3.2], or [5, §2], where the same argument is used for difference sets.) It suffices to determine the structure of the ℓ-Sylow subgroup for each prime ℓ different from p. Such an ℓ is unramified in $\mathbb{Z}[\zeta]$, and (1) can be interpreted as expressing the equivalence of matrices with entries in the localized ring $\mathbb{Z}[\zeta]_{(\ell)}$. This latter ring is a principal ideal domain, and the list of exact powers of ℓ dividing the $\psi(S)$ is precisely the list of elementary divisors of A with respect to the prime ℓ (or ℓ-elementary divisors for short).

By applying the above to each $\ell \neq p$, and noting that r and s are coprime, with $rs = \frac{1-q}{4}$, we obtain the following result:

Theorem 2.1 *The Smith group of* Paley(q) *is isomorphic to* $\mathbb{Z}/2\mu\mathbb{Z} \oplus (\mathbb{Z}/\mu\mathbb{Z})^{2\mu}$, *where* $\mu = \frac{q-1}{4}$.

From the eigenvalues of A, we easily obtain those of $L = kI - A$ (the Laplacian matrix of Paley(q)), namely 0, with multiplicity 1, and $\frac{q+\sqrt{q}}{2}$ and $\frac{q-\sqrt{q}}{2}$, each with multiplicity $\frac{q-1}{2}$. It follows from Kirchhoff's matrix-tree theorem that

$$|K(\mathrm{Paley}(q))| = \frac{1}{q}\left(\frac{q+\sqrt{q}}{2}\right)^k\left(\frac{q-\sqrt{q}}{2}\right)^k = q^{\frac{q-3}{2}}\mu^k,$$

where $\mu = \frac{q-1}{4}$.

The ℓ-elementary divisors of L for primes $\ell \neq p$ can be found in exactly the same way as we found the elementary divisors of A. We can therefore determine the subgroup $K(\mathrm{Paley}(q))_{p'}$ which is complementary to the Sylow p-subgroup of $K(\mathrm{Paley}(q))$.

Theorem 2.2 *Let* $K(\mathrm{Paley}(q)) = K(\mathrm{Paley}(q))_p \oplus K(\mathrm{Paley}(q))_{p'}$ *be the decomposition of the critical group of* Paley(q) *into its Sylow p-subgroup and p-complement. Then* $K(\mathrm{Paley}(q))_{p'} \cong (\mathbb{Z}/\mu\mathbb{Z})^{2\mu}$, *where* $\mu = \frac{q-1}{4}$.

The p-elementary divisors of L remain to be computed, and the rest of the paper is devoted to this task.

3 Character sums and invariants

We will adopt the same notation as in §2. In order to find the p-elementary divisors of L, we will view the entries of L as coming from some p-adic local ring. Let $q = p^t$ and $K = \mathbb{Q}_p(\xi_{q-1})$ be the unique unramified extension of degree t over $\mathbb{Q}_p$, the field of p-adic numbers, where ξ_{q-1} is a primitive $(q-1)^{\text{th}}$ root of unity in K. Let $R = \mathbb{Z}_p[\xi_{q-1}]$ be the ring of integers in K. Then pR is the unique maximal ideal of R and $R/pR \cong \mathbb{F}_q$. Let $T : \mathbb{F}_q^\times \to R^\times$ be the Teichmüller character of $\mathbb{F}_q$. Then T is an R-valued multiplicative character of $\mathbb{F}_q$ of order $q-1$. Hence, T generates the cyclic group $\text{Hom}(\mathbb{F}_q^\times, R^\times)$.

Let $R^{\mathbb{F}_q}$ be the free R-module with basis indexed by the elements of $\mathbb{F}_q$. For clarity, we write the basis element corresponding to $x \in \mathbb{F}_q$ as $[x]$. Then $\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q}$, permuting the basis by field multiplication, so that $R^{\mathbb{F}_q}$ decomposes as the direct sum $R[0] \oplus R^{\mathbb{F}_q^\times}$ of a trivial module with the regular module for $\mathbb{F}_q^\times$.

The regular module $R^{\mathbb{F}_q^\times}$ decomposes further into the direct sum of nonisomorphic $R\mathbb{F}_q^\times$-submodules of R-rank 1, affording the characters T^i, $i = 0, 1, \ldots, q-2$. A basis element for the component affording T^i is

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

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

Next consider the action of the subgroup S of squares in $\mathbb{F}_q^\times$ on $R^{\mathbb{F}_q}$. Then for $0 \leq i \leq q-2$, T^i and T^{i+k} are equal on S. For $0 < i \leq k-1$, let M_i be the R-submodule spanned by $\{e_i, e_{i+k}\}$. Then M_i is the isotypic component for the character $T^i|_S$. The submodule of S-fixed points on $R^{\mathbb{F}_q}$ has basis $\{[0], e_0, e_k\}$, but since $e_0 + [0] = \mathbf{1} = \sum_{x \in \mathbb{F}_q}[x]$, we will use the basis $\{\mathbf{1}, [0], e_k\}$ instead. Let M_0 denote this submodule of R-rank 3. Then we have the decomposition

$$R^{\mathbb{F}_q} = M_0 \oplus M_1 \oplus \cdots \oplus M_{k-1} \qquad (2)$$

We can view A and L as endomorphisms of $R^{\mathbb{F}_q}$, with

$$A([x]) = \sum_{s \in S}[x+s], \ x \in \mathbb{F}_q$$

and

$$L([x]) = k[x] - \sum_{s \in S}[x+s], \ x \in \mathbb{F}_q.$$

Since the action of S preserves adjacency in Paley(q), the maps A and L are RS-module endomorphisms. It follows that A and L map each isotypic component M_i to itself, for $0 \leq i \leq k - 1$, and so they preserve the decomposition (2). Thus, with respect to the basis of $R^{\mathbb{F}_q}$ formed from the bases of the M_i, the matrices of the maps A and L have block diagonal form, with a (2×2)-block for each M_i, for $1 \leq i \leq k - 1$, and a (3×3)-block for M_0. We are therefore reduced to computing the elementary divisors of $L|_{M_i}$ and determining for a given p-power its total multiplicity, as i varies.

The next two lemmas compute L on each of the M_i. The character $T^k = T^{-k}$ of $\mathbb{F}_q^{\times}$ is the quadratic character, and we denote it by χ. Following the convention of Ax [1], T^0 is the character that maps all elements of $\mathbb{F}_q$ to 1, while T^{q-1} maps 0 to 0 and all other elements to 1. Moreover, nonprincipal characters take the value 0 at 0. With these conventions, the characteristic function of S is

$$\frac{1}{2}\left(\chi + T^0 - \delta_0\right),\tag{3}$$

where δ_0 is 1 at 0 and zero elsewhere. Also, we will need Jacobi sums, which we define below. For any two integers a, b, we define the Jacobi sum $J(T^a, T^b)$ by

$$J(T^a, T^b) = \sum_{x \in \mathbb{F}_q} T^a(x) T^b(1 - x).$$

From the above definition and our convention on T^0 and T^{q-1}, we see that if $a \not\equiv 0 \pmod{q - 1}$, then

$$J(T^a, T^0) = 0, \text{ and } J(T^a, T^{q-1}) = -1.$$

Lemma 3.1 *Suppose* $0 \leq i \leq q - 2$ *and* $i \neq 0, k$. *Then*

$$L(e_i) = \frac{1}{2}(q e_i - J(T^{-i}, \chi) e_{i+k})$$

Proof We have

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

$$= \frac{1}{2} \sum_{x \in \mathbb{F}_q^{\times}} T^i(x^{-1}) \sum_{y \in \mathbb{F}_q}\left(\chi(y) + T^0(y) - \delta_0(y)\right)[x + y]$$

$$= \frac{1}{2} \sum_{x \in \mathbb{F}_q^{\times}} T^i(x^{-1}) \sum_{y \in \mathbb{F}_q} \chi(y)[x + y]$$

$$+ \frac{1}{2} \sum_{x \in \mathbb{F}_q^{\times}} T^i(x^{-1}) \sum_{y \in \mathbb{F}_q}[x + y] - \frac{1}{2} \sum_{x \in \mathbb{F}_q^{\times}} T^i(x^{-1})[x].$$

The second sum is zero and the third is $-\frac{1}{2}e_i$. For the first sum, we have

$$\sum_{x\in\mathbb{F}_q^\times} T^i(x^{-1}) \sum_{y\in\mathbb{F}_q} \chi(y)[x+y] = \sum_{z\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q^\times} T^i(x^{-1})\chi(z-x)[z]. \qquad (4)$$

Then if $z \neq 0$, we have $T^i(x^{-1})\chi(z-x) = T^i(z^{-1})\chi(z)T^{-i}((x/z))\chi(1-(x/z))$. The sum over $x \in \mathbb{F}_q^\times$ of these terms is the same as the sum over $x \in \mathbb{F}_q$ and is equal to

$$T^i(z^{-1})\chi(z)J(T^{-i},\chi) = T^{i+k}(z^{-1})J(T^{-i},\chi).$$

If $z = 0$, then $\sum_{x\in\mathbb{F}_q^\times} T^i(x^{-1})\chi(-x) = 0$. Thus, the outer sum over all $z \in \mathbb{F}_q$ can be taken over $\mathbb{F}_q^\times$ and is equal to $J(T^{-i},\chi)e_{i+k}$. The lemma now follows since $L = kI - A$. $\square$

Lemma 3.2 *(i)* $L(\mathbf{1}) = 0$.
(ii) $L(e_k) = \frac{1}{2}(\mathbf{1} - q([0] - e_k))$.
(iii) $L([0]) = \frac{1}{2}(q[0] - e_k - \mathbf{1})$.

Proof (i) is obvious, and (iii) is straightforward. (ii) is proved by the same calculation as in the previous lemma, using the fact that $J(\chi,\chi) = -\chi(-1) = -1$. The only difference in the calculation is that in the equation (4), the $z = 0$ term is $(q-1)[0]$ instead of zero. $\square$

Corollary 3.3 *The Laplacian matrix L is equivalent over R to the diagonal matrix with diagonal entries $J(T^{-i}, T^k)$, for $i = 1, \ldots, q-2$ and $i \neq k$, two 1s, and one zero.*

In view of Corollary 3.3, to compute the p-elementary divisors of L, we will need to know the p-adic valuations of Jacobi sums. Using Stickelberger's theorem on Gauss sums [16] (see [7, p. 636] for further reference) and the well-known relation between Gauss and Jacobi sums, we have

Theorem 3.4 *Let a and b be integers such that $a \not\equiv 0 \pmod{q-1}$, $b \not\equiv 0 \pmod{q-1}$, and $a+b \not\equiv 0 \pmod{q-1}$. For any integer x, we use $s(x)$ to denote the sum of digits in the expansion of the least nonnegative residue of x modulo $(q-1)$ as a base p number. Then*

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

where $v_p(J(T^{-a}, T^{-b}))$ is the p-adic valuation of $J(T^{-a}, T^{-b})$. In other words, the number of times that p divides $J(T^{-a}, T^{-b})$ is equal to the number of carries in the addition $a+b \pmod{q-1}$.

By Theorem 3.4, the p-adic valuation of $J(T^{-i}, T^k)$ for $i \neq k$ is known to be equal to $c(i) := \frac{1}{p-1}(s(i) + \frac{t(p-1)}{2} - s(i+k))$, since $s(k) = \frac{t(p-1)}{2}$. The number $c(i)$

can be interpreted as the number of carries, when adding the p-expansions of i and k, modulo $q - 1$. This will be formulated precisely in the next section. It is already clear that there are no elementary divisors of L greater than p^t. It is also easy to see that the p-rank of L (i.e., the number of times that p^0 appears as an elementary divisor of L) equals $(\frac{p+1}{2})^t$, since a necessary and sufficient condition for there to be no carries is that each of the p-digits of i be in the range from 0 to $\frac{p-1}{2}$. This was already shown by Brouwer and van Eijl [4, p.336]. Also, since $c(i) + c(q - 1 - i) = t$, it follows from Corollary 3.3 that the multiplicity of p^t as an elementary divisor is $(\frac{p+1}{2})^t - 2$. It remains to find the multiplicity of p^λ for $1 \leq \lambda \leq t - 1$. In order to find the multiplicity of p^λ as an elementary divisor of L, we have to count the number of i ranging from 1 to $q - 2$, $i \neq k$, such that adding i to k involves exactly λ carries.

4 The counting problem

In order to finish our computations of the critical groups of Paley(q), we will solve the following counting problem using the transfer matrix method. For a discussion of the transfer matrix method and its various applications, we refer the reader to [15, Section 4.7].

The counting problem. Let $q = p^t$ be an odd prime power and $k = \frac{q-1}{2}$. For $1 \leq \lambda \leq t - 1$, what is the number of i, $1 \leq i \leq q - 2$, $i \neq k$ such that adding i to $\frac{q-1}{2}$ modulo $q - 1$ involves exactly λ carries?

We express integers a, $0 \leq a \leq q - 1$, in base p. That is, we write

$$a = a_{t-1}p^{t-1} + a_{t-2}p^{t-2} + \cdots + a_1 p + a_0,$$

where $0 \leq a_i \leq p - 1$ for all i. In what follows, we will simply write $a = a_{t-1}a_{t-2} \cdots a_1 a_0$, and call the a_i's the digits of a. Since we are going to add a with $\frac{q-1}{2}$ modulo $q - 1$, we will use the modular p-ary add-with-carry algorithm described in [8, Theorem 4.1]. Let $a = a_{t-1}a_{t-2} \cdots a_1 a_0$ and $b = b_{t-1}b_{t-2} \cdots b_1 b_0$ be integers in $\{1, 2, \ldots, q - 2\}$ such that $a + \frac{q-1}{2} = b$ modulo $q - 1$. By the modular p-ary add-with-carry algorithm (cf. [8, Theorem 4.1]), there is a unique *carry sequence* $c = c_{t-1}c_{t-2} \cdots c_1 c_0$ with $c_i \in \{0, 1\}$ and $c_t = c_0$ such that for all $0 \leq i \leq t - 1$,

$$a_i + \frac{p - 1}{2} + c_i = b_i + p c_{i+1}. \tag{5}$$

By the number of carries, we shall mean the number of i with $c_i = 1$.

We will use the transfer matrix method to solve the above counting problem. This approach involves constructing a weighted digraph G, and changing the counting problem to that of counting closed walks in G of certain length and weight. The above equations motivate us to construct the digraph G on $[p] \times [2]$ (here $[p] = \{0, 1, \ldots, p - 1\}$ and $[2] = \{0, 1\}$) as follows: The vertices of G are $(\alpha, \gamma) \in [p] \times [2]$. There is an arc from (α, γ) to (α', γ') if and only if

$$\alpha + \frac{p-1}{2} + \gamma = \beta + p\gamma' \tag{6}$$

for some $\beta \in [p]$. Furthermore, if there is an arc e from (α, γ) to (α', γ'), then we give the arc label α and weight $w(e) := \gamma'$. By the weight of a walk in the digraph, we shall mean the sum of the weights of its arcs. Each walk of length t in G specifies an element $a = a_{t-1}a_{t-2}\cdots a_0 \in \{0, 1, \ldots, q-1\}$ by taking the first arc label to be a_0, the second to be a_1, etc. In terms of the digraph G, the discussion leading up to equation (5) means that for each $a \in \{1, \ldots, q-2\} \setminus \{\frac{q-1}{2}\}$, there is a unique closed walk of length t in G whose arc labels specify a, and that the weight of this walk is equal to the number of carries when adding $\frac{q-1}{2}$ to a modulo $q-1$. There are some other closed walks of length t in G, namely those whose arc labels specify $a = 0$, $\frac{q-1}{2}$, or $q-1$. We must check that these walks have weights which are outside the range $\{1, 2, \ldots, t-1\}$ for λ in our counting problem. Once we have checked this, we will know that our counting problem is equivalent to counting, for each $1 \le \lambda \le t-1$, the closed walks of length t, and weight λ in G. If $a = 0$, then $a_i = 0$ for all i, and there is just one closed walk, of weight 0. If $a = q-1$, then $a_i = p-1$ for all i, and there is again just one closed walk, of weight t. Finally, for $a = \frac{q-1}{2}$, there are two closed walks one of weight 0, where in equation (6) we take $\alpha = \frac{p-1}{2}$, $\beta = p-1$, and $\gamma = 0$ for every arc, and the other of weight t, where we take $\alpha = \frac{p-1}{2}$, $\beta = 0$, and $\gamma = 1$ for every arc.

Let B be the adjacency matrix of the digraph G. More precisely, the rows and columns of B are both indexed by $(\alpha, \gamma) \in [p] \times [2]$, and the entry $((\alpha, \gamma), (\alpha', \gamma'))$ of B is 0 if there is no arc from (α, γ) to (α', γ'); it is 1 if there is an arc e from (α, γ) to (α', γ') and $w(e) = 0$; and it is x if there is an arc e from (α, γ) to (α', γ') and $w(e) = 1$ (here x is an indeterminate). Note that since (6) does not involve α', the adjacency matrix B has only two distinct rows, each repeated p times. More explicitly,

$$
B = \begin{array}{c}
\frac{p+1}{2}\left\{\begin{array}{c}\\ \\ \\ \end{array}\right. \\
\frac{p-1}{2}\left\{\begin{array}{c}\\ \\ \\ \end{array}\right. \\
\frac{p-1}{2}\left\{\begin{array}{c}\\ \\ \\ \end{array}\right. \\
\frac{p+1}{2}\left\{\begin{array}{c}\\ \\ \\ \end{array}\right.
\end{array}
\begin{pmatrix}
\overbrace{\begin{matrix}1 & \cdots & 1\end{matrix}}^{p} & \overbrace{\begin{matrix}0 & \cdots & 0\end{matrix}}^{p} \\
\vdots & \vdots & \vdots & \vdots \\
1 & \cdots & 1 & 0 & \cdots & 0 \\
0 & \cdots & 0 & x & \cdots & x \\
\vdots & \vdots & \vdots & \vdots \\
0 & \cdots & 0 & x & \cdots & x \\
1 & \cdots & 1 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots \\
1 & \cdots & 1 & 0 & \cdots & 0 \\
0 & \cdots & 0 & x & \cdots & x \\
\vdots & \vdots & \vdots & \vdots \\
0 & \cdots & 0 & x & \cdots & x
\end{pmatrix}
$$

If $\Psi = e_1 e_2 \cdots e_n$ is a walk in G, we define $\mathrm{wt}(\Psi) = x^{w(e_1)+w(e_2)+\cdots+w(e_n)}$. Let

$$C_G(n) = \sum_{\Psi} \mathrm{wt}(\Psi),$$

where the sum is extended over all closed walks of length n in G. Then $C_G(n) = \sum_{m \geq 0} f(n, m) x^m$, where $f(n, m)$ is the number of closed walks of length n and weight m. Let

$$F(z, x) = \sum_{n \geq 1} C_G(n) z^n.$$

By Corollary 4.7.3 of [15, p. 501], we have

$$F(z, x) = -\frac{z \frac{\partial Q(z, x)}{\partial z}}{Q(z, x)},$$

where $Q(z, x) = \det(I - zB)$. Using the above definition of B, we find that $\det(I - zB) = 1 - \frac{p+1}{2}(1 + x)z + pxz^2$. It follows that

$$F(z, x) = \frac{U - 2V}{1 - U + V} = \frac{(U - V) - V}{1 - (U - V)},$$

with $U = \frac{p+1}{2}(1 + x)z$ and $V = pxz^2$. Extracting the coefficient of $x^m z^n$ in $F(z, x)$, we obtain

$$f(n, m) = \sum_i \frac{n}{n - i} \binom{n - i}{i} \binom{n - 2i}{m - i} (-p)^i \left(\frac{p + 1}{2} \right)^{n - 2i}.$$

Notice that $f(n, m) = f(n, n - m)$.

Summing up, we have the following:

Theorem 4.1 *Let $q = p^t$ be a prime power congruent to 1 modulo 4. Then the number of p-adic elementary divisors of $L(\mathrm{Paley}(q))$, which are equal to p^λ, $0 \leq \lambda < t$, is*

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

The number of p-adic elementary divisors of $L(\mathrm{Paley}(q))$ which are equal to p^t is $\left(\frac{p+1}{2} \right)^t - 2$.

Example 4.2 In [11], $K(\mathrm{Paley}(25))$ is calculated directly by a computer. Here as an illustration of Theorem 4.1, we use the above formula to compute $K(\mathrm{Paley}(5^3))$ and $K(\mathrm{Paley}(5^4))$:

$$f(3, 0) = 3^3 = 27.$$

$$f(3, 1) = \binom{3}{1} \cdot 3^3 - \frac{3}{2} \binom{2}{1} \binom{1}{0} \cdot 5 \cdot 3 = 36.$$

Therefore,

$$K(\mathrm{Paley}(5^3)) \cong (\mathbb{Z}/31\mathbb{Z})^{62} \oplus (\mathbb{Z}/5\mathbb{Z})^{36} \oplus (\mathbb{Z}/25\mathbb{Z})^{36} \oplus (\mathbb{Z}/125\mathbb{Z})^{25}.$$

$$f(4, 0) = 3^4 = 81.$$

$$f(4, 1) = \binom{4}{1} \cdot 3^4 - \frac{4}{3}\binom{3}{1}\binom{2}{0} \cdot 5 \cdot 3^2 = 144.$$

$$f(4, 2) = \binom{4}{2} \cdot 3^4 - \frac{4}{3}\binom{3}{1}\binom{2}{1} \cdot 5 \cdot 3^2 + \frac{4}{2}\binom{2}{2}\binom{0}{0} \cdot 5^2 = 176.$$

Therefore,

$$K(\mathrm{Paley}(5^4)) \cong (\mathbb{Z}/156\mathbb{Z})^{312} \oplus (\mathbb{Z}/5\mathbb{Z})^{144} \oplus (\mathbb{Z}/25\mathbb{Z})^{176} \oplus (\mathbb{Z}/125\mathbb{Z})^{144}$$
$$\oplus (\mathbb{Z}/625\mathbb{Z})^{79}.$$

References

1. Ax, J.: The zeroes of polynomials over finite fields. Am. J. Math. **86**, 255–261 (1964)
2. Biggs, N.L.: Chip-firing and the critical group of a graph. J. Algebr. Comb. **9**(1), 25–45 (1999)
3. Brouwer, A.E., Haemers, W.H.: Spectra of Graphs. Universitext. Springer, New York (2012)
4. Brouwer, A.E., van Eijl, C.A.: On the p-rank of the adjacency matrices of strongly regular graphs. J. Algebr. Comb. **1**(4), 329–346 (1992)
5. Chandler, D.B., Xiang, Q.: The invariant factors of some cyclic difference sets. J. Comb. Theory Ser. A **101**(1), 131–146 (2003)
6. Dhar, D.: Self-organized critical state of sandpile automaton models. Phys. Rev. Lett. **64**(14), 1613–1616 (1990)
7. Dwork, B.: On the rationality of the zeta function of an algebraic variety. Am. J. Math. **82**, 631–648 (1960)
8. Helleseth, T., Hollmann, H.D.L., Kholosha, A., Wang, Z., Xiang, Q.: Proofs of two conjectures on ternary weakly regular bent functions. IEEE Trans. Inf. Theory **55**(11), 5272–5283 (2009)
9. Levine, L., Propp, J.: What is.. a sandpile? Not. Am. Math. Soc. **57**(8), 976–979 (2010)
10. Lorenzini, D.: Arithmetical graphs. Math. Ann. **285**(3), 481–501 (1989)
11. Lorenzini, D.: Smith normal form and Laplacians. J. Comb. Theory Ser. B **98**(6), 1271–1300 (2008)
12. MacWilliams, F.J., Mann, H.B.: On the p-rank of the design matrix of a difference set. Inf. Control **12**, 474–488 (1968)
13. Rushanan, J.J.: Topics in integral matrices and abelian group codes, ProQuest LLC, Ann Arbor, Ph.D. Thesis, California Institute of Technology (1986)
14. Sin, P.: Smith normal forms of incidence matrices. Sci. China Math. **56**(7), 1359–1371 (2013)
15. Stanley, R.P.: Enumerative Combinatorics. Vol. 1, second edition. In: Cambridge Studies in Advanced Mathematics, vol. 49. Cambridge University Press, Cambridge (2012)
16. Stickelberger, L.: Ueber eine Verallgemeinerung der Kreistheilung. Math. Ann. **37**(3), 321–367 (1890)