J Algebr Comb (2009) 30: 255–276
DOI 10.1007/s10801-008-0162-z

The critical groups of a family of graphs and elliptic curves over finite fields

Gregg Musiker

Received: 9 October 2007 / Accepted: 3 November 2008 / Published online: 28 November 2008

Abstract Let q be a power of a prime, and E be an elliptic curve defined over $\mathbb{F}_q$. Such curves have a classical group structure, and one can form an infinite tower of groups by considering E over field extensions $\mathbb{F}_{q^k}$ for all $k \geq 1$. The critical group of a graph may be defined as the cokernel of $L(G)$, the Laplacian matrix of G. In this paper, we compare elliptic curve groups with the critical groups of a certain family of graphs. This collection of critical groups also decomposes into towers of subgroups, and we highlight additional comparisons by using the Frobenius map of E over $\mathbb{F}_q$.

Keywords Elliptic curves · Critical group · Graph Laplacian · Frobenius map

1 Introduction

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, where q is a power of the prime p, and let $\overline{\mathbb{F}_p}$ denote the algebraic closure of $\mathbb{F}_p$. Recall that the abelian group $E(\overline{\mathbb{F}_p})$ is endowed with a group homomorphism π, called the Frobenius map, which satisfies the relation $\pi^2 - (1 + q - N_1)\pi + q = 0$, where $N_1 = |E(\mathbb{F}_q)|$. For each k, the subgroup $E(\mathbb{F}_{q^k})$ is equal to the kernel of $1 - \pi^k$. The integer N_1 completely determines the integers $N_k := |E(\mathbb{F}_{q^k})|$.

In this paper, we define a purely analogous combinatorial structure. More precisely, we define wheels graphs $W_k(q, t)$ for various allowed integers (q, k, t). By taking the cokernels of the associated Laplacian matrices, to each such graph we attach an abelian group $K(W_k(q, t))$, called the critical group of the graph, which we

This work was partially supported by the NSF, grant DMS-0500557 during the author's graduate school at the University of California, San Diego, and partially supported by an NSF Postdoctoral Fellowship.

G. Musiker (✉)
Mathematics Department, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
e-mail: musiker@math.mit.edu

abbreviate as $K(q,k,t)$. When $k_1 \mid k_2$, we define a natural injective group homomorphism $K(q,k_1,t) \to K(q,k_2,t)$ (Proposition 3.2). Using these injective group homomorphisms, one defines in a natural way its direct limit, an abelian group that we denote by $\overline{K}(q,t)$. We then define on $\overline{K}(q,t)$ an endomorphism ρ, called the shift map, which satisfies the equation $\rho^2 - (1+q-t)\rho + q = 0$ (Theorem 4.4), and such that the kernel of $1-\rho^k$ is the natural subgroup of $\overline{K}(q,t)$ corresponding to $K(q,k,t)$ (Theorem 3.6). Furthermore, it is a standard fact in the theory of elliptic curves that two elements suffice to generate $E(\mathbb{F}_{q^k})$. The groups $K(q,k,t)$ enjoy the same property (Theorem 5.1). It is also true that for any positive integer n, the group $E(\overline{\mathbb{F}_p})$ contains a torsion subgroup $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if and only if n and q are coprime. Further, an elliptic curve E is *ordinary* if and only if $E(\overline{\mathbb{F}_p})$ contains $\mathbb{Z}/p\mathbb{Z}$. It will develop (Theorem 5.10) that $\overline{K}(q,t)$ has both of these properties too.

The proofs of these group theoretic properties are completely combinatorial. In fact they are a consequence of explicit formulas that we obtain for the group presentations of the $K(q,k,t)$'s (Corollary 5.2). We extend this result to a larger family of matrices (Theorem 5.7), thus generalizing a cyclicity result of N. Biggs (Remark 5.6).

The relationship between the combinatorial structure introduced by the author and elliptic curves is even tighter. Fix an integer k. The order of the group $K(q,k,t)$ is then given by the evaluation of a polynomial of degree k in Q and T (Theorem 2.1), denoted by $\mathcal{W}_k(Q,T)$. The graphs $W_k(q,t)$ were chosen so that the following additional relation holds for any power of a prime q and any ellptic curve $E/\mathbb{F}_q$:

$$N_k = -\mathcal{W}_k(q,t) \quad \text{(Theorem 2.3)}.$$

By convention, we use q here to be a fixed power of a prime, so that the cardinality of $E(\mathbb{F}_q)$ is a specific integer rather than a polynomial. To make this clearer, we will reserve capital letters for the arguments of our formulas when we want to emphasize their properties as polynomials. However, most of the time, we will be assuming that a fixed q and t have been chosen, and that the expressions encountered throughout this paper are integers.

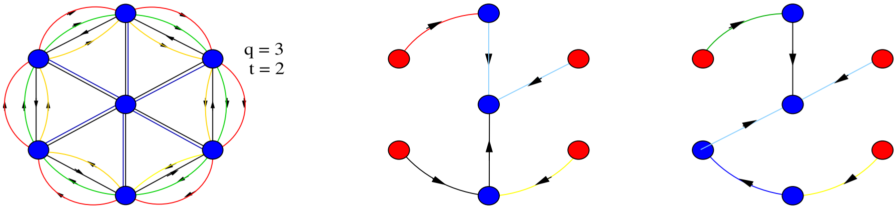
The factorization over $\mathbb{Z}$ of the polynomial $\mathcal{W}_k(Q,T)$ into a product of irreducibles is given in Theorem 4.1 via bipartite analogues of cyclotomic polynomials. As we prove in Theorem 4.2, the evaluation of these bivariate polynomials has a combinatorial interpretation in terms of the groups $\{K(q,k,t)\}$.

As a final application, we obtain group presentations for elliptic curves E over finite fields that have endomorphism rings isomorphic to $\mathbb{Z}[\pi]$ (Theorem 5.13). We show that for such E, the group $E(\overline{\mathbb{F}_p})$ can be described as a direct limit of matrix cokernels, analogous to $\overline{K}(q,t)$ (Corollary 5.14).

2 An enumerative correspondence between elliptic curves and wheel graphs

Let W_k denote the kth wheel graph, which consists of $(k+1)$ vertices, k of which lie in a cycle and are each adjacent to the last vertex. (We also define W_k analogously in the case $k=1$ or $k=2$: W_1 is a graph on two vertices, v_0 and v_1, with a loop at v_1 and a single edge between v_0 and v_1. Graph W_2 has three vertices, v_0, v_1, and v_2, with two edges from v_1 to v_2, a single edge between v_0 and v_1, and one edge between v_0 and v_2.) Using the W_k's, we define the (q,t)-wheel graph with $(k+1)$ vertices, which we denote as $W_k(q,t)$, to be the following directed graph with multiple edges (digraph). We use the 0-skeleton of the wheel graph W_k, where we label the central vertex as v_0, and the vertices on the rim as v_1 through v_k in clockwise order. We then attach t bi-directed spokes between v_0 and v_i for all $i \in \{1,2,\dots,k\}$. Additionally, we attach a single counter-clockwise edge between v_i and v_{i-1} (working modulo k) for each vertex on the rim. Finally, we attach q clockwise edges between v_i and v_{i+1} (again working modulo k). As degenerate cases, the (q,t)-wheel graph $W_1(q,t)$ has $(q+1)$ loops at vertex v_1 and t bi-directed edges between v_0 and v_1. The graph $W_2(q,t)$ has $(q+1)$ edges directed from v_1 to v_2, $(q+1)$ edges directed from v_2 to v_1, t bi-directed edges from v_0 and v_1, and t bi-directed edges from v_0 to v_2.

A directed spanning tree of a digraph G with root v_0 is a connected subgraph containing all vertices of G, which does not contain any cycles, and has all edges directed inward toward v_0. In the case of these digraph analogues of wheel graphs, a directed spanning tree is easily defined as a collection of disconnected arcs on the rim, which each connect to the central hub along one spoke for each arc.



The (q,t)-wheel graph $W_6(3,2)$ and two of its directed spanning trees.

Theorem 2.1 *For each integer $k \geq 1$, there exists a bivariate polynomial in q and t of degree k, which we denote by $\mathcal{W}_k(Q,T)$, such that the following property holds: for all $q \geq 0$ and $t \geq 1$, the number of directed spanning trees of digraph $W_k(q,t)$ equals the evaluation $\mathcal{W}_k(Q,T)|_{Q=q,T=t}$, which we abbreviate as $\mathcal{W}_k(q,t)$.*

For the proof of this result, we must first define the Laplacian matrix of a digraph. The Laplacian $L(G)$ of a digraph G on m vertices, with possibly multiple edges, is defined to be the m-by-m matrix in which off-diagonal entries $L_{ij} = -d(i,j)$ and diagonal entries $L_{ii} = d(i)$. Here $d(i,j)$ is the number of edges from v_i to v_j, and $d(i)$ is the outdegree of vertex v_i, or more simply we choose L_{ii} such that each row of L sums to zero.

Proof We appeal to the directed multi-graph version of the Matrix-Tree Theorem [15, pg. 58] to count the number of spanning trees of $W_k(q,t)$ with the root at the hub. The Matrix-Tree Theorem states that the number of spanning trees of G on vertices $\{v_1, v_2, \dots, v_m\}$ with the hub v_i is given by $\det L_0(G)$ where $L_0(G)$ is the matrix $L(G)$ with the ith row and ith column deleted.

In the case of $W_k(q,t)$, the Laplacian matrix is the $(k+1)$-by-$(k+1)$ matrix

$$L(W_k(q,t)) = \begin{bmatrix} 1+q+t & -q & 0 & \dots & 0 & -1 & -t \\ -1 & 1+q+t & -q & 0 & \dots & 0 & -t \\ \dots & \dots & \dots & \dots & \dots & \dots & -t \\ 0 & \dots & -1 & 1+q+t & -q & 0 & -t \\ 0 & \dots & 0 & -1 & 1+q+t & -q & -t \\ -q & 0 & \dots & 0 & -1 & 1+q+t & -t \\ -t & -t & -t & \dots & -t & -t & kt \end{bmatrix}$$

where the last row and column correspond to the hub vertex. Thus the number of directed spanning trees rooted at the hub is the determinant of $L_0(W_k(q,t))$, the matrix formed by deleting the last row and column from $L(W_k(q,t))$. Since we will encounter this matrix throughout this paper, we let $\overline{M}_k$ denote this reduced Laplacian, i.e.

$$\overline{M}_k = \begin{bmatrix} 1+q+t & -q & 0 & \dots & 0 & -1 \\ -1 & 1+q+t & -q & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & -1 & 1+q+t & -q & 0 \\ 0 & \dots & 0 & -1 & 1+q+t & -q \\ -q & 0 & \dots & 0 & -1 & 1+q+t \end{bmatrix}.$$

The determinant of $\overline{M}_k$ is a bivariate polynomial of degree k, and thus so is the number of directed spanning trees of $W_k(q,t)$ rooted at the hub. □

Remark 2.2 In fact, the coefficients appearing in the polynomial $\mathcal{W}_k(Q,T)$ are not only integers, but are *positive* integers, as we explain below.

The family of polynomials $\{\mathcal{W}_k(Q,T)\}$ also yield formulas for enumerating the number of points on an elliptic curve over a finite field $\mathbb{F}_{q^k}$.

Theorem 2.3 *For all powers of a prime, q, the number of points on an elliptic curve E over a finite field $\mathbb{F}_{q^k}$, which we denote by N_k, satisfies the identity*

$$N_k = -\mathcal{W}_k(Q,T)|_{Q=q,T=-N_1},$$

where $N_1 = \#E(\mathbb{F}_q)$ and $\mathcal{W}_k(Q,T)$ is the polynomial defined by Theorem 2.1.

The proof of Theorem 2.3 follows from the author's work in [12]. In particular, this theorem appeared there as Theorem 3 with a slightly different but equivalent definition of $\mathcal{W}_k(Q,T)$. To see the equivalence, we simply note that we have multiple edges in digraph $W_k(q,t)$ whenever we previously had a weight in generating function $\mathcal{W}_k(Q,T)$. Based on this generating function interpretation of $\mathcal{W}_k(Q,T)$ from [12], we are able to conclude that the coefficients of $\mathcal{W}_k(Q,T)$ are positive. On the other hand, an application of this new characterization of $\mathcal{W}_k(Q,T)$ is another proof of the determinantal formula for N_k which appeared in [12].

Define the family of matrices M_k by $M_1 = [-N_1]$, $M_2 = \begin{bmatrix} 1+q-N_1 & -1-q \\ -1-q & 1+q-N_1 \end{bmatrix}$, and for $k \geq 3$, let M_k be the k-by-k "three-line" circulant matrix

$$\begin{bmatrix} 1+q-N_1 & -q & 0 & \dots & 0 & -1 \\ -1 & 1+q-N_1 & -q & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & -1 & 1+q-N_1 & -q & 0 \\ 0 & \dots & 0 & -1 & 1+q-N_1 & -q \\ -q & 0 & \dots & 0 & -1 & 1+q-N_1 \end{bmatrix}.$$

Theorem 2.4 (Theorem 5 in [12]) *The sequence of integers $N_k := \#E(\mathbb{F}_{q^k})$ satisfies the relation*

$$N_k = -\det M_k$$

for all $k \geq 1$.

Proof Starting with the identity of Theorem 2.3 and using the determinantal formula for $\mathcal{W}_k(q,t)$ from the proof of Theorem 2.1, we obtain the identities

$$\begin{aligned} N_k &= -\mathcal{W}_k(Q,T)|_{Q=q,T=-N_1}, \\ M_k &= \overline{M}_k\Big|_{t=-N_1}, \quad \text{and thus} \\ \mathcal{W}_k(q,t) &= \det(\overline{M}_k) \text{ implies} \\ -\mathcal{W}_k(q,-N_1) &= -\det(\overline{M}_k)\Big|_{t=-N_1}, \text{ so we get} \\ N_k &= -\det M_k. \end{aligned}$$

Thus we have proven Theorem 2.4. □

We will return to ramifications of this combinatorial identity in Section 2, after discussing another instance of the graph Laplacian.

3 Critical groups of graphs and maps between them

In this section, we discuss critical groups on graphs. Critical groups of graphs have appeared previously in the literature, often with different names. These have been studied in connection to chip-firing games by Biggs [2]; are also known as abelian sandpile groups as described by Dhar [5] and Gabrielov [6]; and have been studied by Lorenzini in [9] where they were called the group of components. Connections to curves also appear in work of Baker and Norine [1] where they extend the notion of rank for linear systems of curves to the case of graphs. They subsequently obtain a Riemann-Roch Theorem for critical groups of graphs, also referred to as Jacobians.

The critical group of a graph G, denoted as $K(G)$, can be simply defined by the cokernel of the transpose of the reduced Laplacian:

$$K(G) \cong \text{ coker } L_0(G) = \mathbb{Z}^k / \operatorname{Im} L_0^T(G).$$

In particular, for any graph G, $|K(G)| = |\det L_0(G)| =$ the number of directed spanning trees of G. This quantity is known as the graph's complexity, and enumerates other important features of a graph G, such as the number of G-parking functions, as observed by Postnikov and Shapiro [13]. Critical groups were originally defined for undirected graphs, but David Wagner [16] generalized this definition to digraphs as the cokernel of the transpose of the Laplacian.

In the remainder of this paper, we use Theorem 2.4 to extend the numerical identity of Theorem 2.3 to a comparison of the groups $\{E(\mathbb{F}_{q^k})\}_{k=1}^{\infty}$ and $\{K(W_k(q,t))\}_{k=1}^{\infty}$. As noted in the introduction, we henceforth abbreviate the critical group of the (q,t)-wheel graph, $K(W_k(q,t))$, as $K(q,k,t)$.

One of the fundamental properties of an elliptic curve over a finite field is the existence of the Frobenius map. In particular, for a finite field $\mathbb{F}_q$, where $q = p^k$, p prime, the Galois group $\operatorname{Gal}(\mathbb{F}_{q^\ell}/\mathbb{F}_q)$ is a cyclic group generated by the map $\pi : x \mapsto x^q$. The Frobenius map π acts on an elliptic curve defined over $\mathbb{F}_q$, by raising a points' coordinates to the qth powers. In particular, we let $\overline{\mathbb{F}_p}$ denote the algebraic closure of $\mathbb{F}_q$ (q is a power of prime p). For example, if we have a planar affine model for our curve,

$$\begin{aligned} \pi : E(\overline{\mathbb{F}_p}) &\to E(\overline{\mathbb{F}_p}) \\ (x,y) &\mapsto (x^q, y^q). \end{aligned}$$

An elliptic curve can be given a group structure after choosing a $\mathbb{F}_q$-rational point, such as the point at infinity, as the identity. For example see [14, pg. 55].

Lemma 3.1

$$\begin{aligned} &\pi(P \oplus Q) = \pi(P) \oplus \pi(Q), \\ &\pi^k(P) = P \textit{ if and only if} P \in E(\mathbb{F}_{q^k}), \quad \textit{and, then} \end{aligned}$$

$$E(\mathbb{F}_q) \subset E(\mathbb{F}_{q^{k_1}}) \subset E(\mathbb{F}_{q^{k_2}}) \subset E(\mathbb{F}_{q^{k_3}}) \subset \cdots \subset E(\overline{\mathbb{F}_p})$$

whenever we have the divisibilities $k_1|k_2$, $k_2|k_3$, *and so on.*

Proof See Section 4.2 of [18]. □

Our goal now is to understand the sequence of $\{K(q,k,t)\}_{k=1}^{\infty}$ in a way that corresponds to the chain

$$E(\mathbb{F}_q) \subset E(\mathbb{F}_{q^{k_1}}) \subset E(\mathbb{F}_{q^{k_2}}) \subset E(\mathbb{F}_{q^{k_3}}) \subset \cdots \subset E(\overline{\mathbb{F}_p})$$

for $k_1|k_2|k_3$, etc.

Let ψ_{k_2,k_1} denote the map represented by the k_2-by-k_1 matrix constructed by vertically repeating the k_1-by-k_1 identity matrix (k_2/k_1) times. We also use the notation $\overline{M}_k^T$ for the transpose of the reduced Laplacian matrix of the digraph $W_k(q,t)$ with root vertex given by the central hub and vertices on the rim labeled in clockwise order. In other words, $\overline{M}_k^T$ is the k-by-k circulant matrix with the first row given by $[1+q+t,-1,0,\dots,0,-q]$.

Proposition 3.2 *For any integers $q \geq 0, t \geq 1, k_1 \geq 1, k_2 \geq 1$ such that $k_1|k_2$, the map ψ_{k_2,k_1} is an injective group homomorphism between $K(q,k_1,t)$ and $K(q,k_2,t)$.*

We postpone this proof until later in this section, after the statement of Proposition 3.3. Define ρ_k to be the rotation map on $K(q,k,t)$. Here we consider elements of the critical group to be column vectors in $\mathbb{Z}^k/\operatorname{Im}\overline{M}_k^T$ which encode an assignment of an integer to each vertex on the rim of $W_k(q,t)$. We define ρ_k to circularly rotate the vectors downward, which corresponds to rotating the rim vertices of W_k clockwise. Observe that for all $k \geq 1$, ρ_k and the addition in $K(q,k,t)$ commute.

Proposition 3.3 *Under the same hypotheses as in Proposition 3.2, the kernel of* $(1-{\rho_{k_2}}^{k_1})$ *acting on $K(q,k_2,t)$ is the subgroup $K(q,k_1,t)$.*

Proof We prove both of these propositions simultaneously. Because of the periodic nature of the circulant $\overline{M}_k^T$'s, we have the identity

$$\psi_{k_2,k_1} \circ \overline{M}_{k_1}^T = \overline{M}_{k_2}^T \circ \psi_{k_2,k_1}.$$

Thus if $v \in \mathbb{Z}^{k_1}$ satisfies $v \in \operatorname{Im}\overline{M}_{k_1}^T$, then $\psi_{k_2,k_1}(v) \in \operatorname{Im}\overline{M}_{k_2}^T$. Additionally, since $\overline{M}_{k_2}^T$ is nonsingular, the equation

$$\overline{M}_{k_2}^T[x_1 - x_{1+k_1}, x_2 - x_{2+k_1}, \dots, x_{k_2} - x_{0+k_1}]^T = 0$$

only has the zero vector as a solution. In other words, if $[v,v,\dots,v]^T \in \operatorname{Im}\overline{M}_{k_2}^T$ with $[v,v,\dots,v]^T = \overline{M}_{k_2}^T[x_1,x_2,\dots,x_{k_2}]^T$, then the sequence of x_i's is (k_1)-periodic, hence $[v,v,\dots,v]^T \in \operatorname{Im}\overline{M}_{k_2}^T \circ \psi_{k_2,k_1}$.

Consequently, we get the reverse implication, i.e. $\psi_{k_2,k_1}(v) \in \operatorname{Im}\overline{M}_{k_2}^T$ if and only if $v \in \operatorname{Im}\overline{M}_{k_1}^T$. Since $K(q,k,t)$ is defined as $\mathbb{Z}^k/\operatorname{Im}\overline{M}_k^T$, the proof of Proposition 3.2 is complete. We have also completed the proof of Proposition 3.3 since we have shown that $K(q,k_1,t)$ is a subgroup of $K(q,k_2,t)$ when $k_1|k_2$ and that this subgroup is the set of (k_1)-periodic vectors. □

Lemma 3.4 *For all $k_1,k_2,k_3 \geq 1$ with $k_1|k_2$ and $k_2|k_3$,*

$$\psi_{k_3,k_1} = \psi_{k_3,k_2} \circ \psi_{k_2,k_1} : K(q,k_1,t) \to K(q,k_3,t).$$

Proof ψ_{k_3,k_2} is the k_3-by-k_2 matrix with I_{k_2} repeated k_3/k_2 times. Thus $\psi_{k_3,k_2} \circ \psi_{k_2,k_1}$ is the k_3-by-k_1 matrix formed by repeating ψ_{k_2,k_1} k_3/k_2 times. This resulting matrix has the identity matrix I_{k_1} repeated $(k_3/k_2)(k_2/k_1) = k_3/k_1$ times. □

We therefore can define the direct limit of the set $\{K(q,k,t)\}_{k=1}^{\infty}$ using partial order $k_1 \prec k_2$ iff $k_1|k_2$ and using the $\psi_{k_2,k_1} : K(q,k_1,t) \to K(q,k_2,t)$ as our transition maps. Furthermore, since ψ_{k_2,k_1} are all injective, we can naturally identify each $K(q,k,t)$ as a subgroup of

$$\overline{K}(q,t) := \varinjlim_{k\geq 1}\{K(q,k,t)\}.$$

Consequently, we can alternatively define $\overline{K}(q,t)$ as the set of periodic vectors

$$w = (\ldots, w_{-3}, w_{-2}, w_{-1}, w_0, w_1, w_2, w_3, \ldots) \in \{0, 1, 2, \ldots, q+t\}^{\mathbb{Z}}$$

such that when w is the periodic extension of fundamental subword $(w_1, w_2, \ldots, w_k)$, then $[w_1, w_2, \ldots, w_k]^T \in K(q,k,t)$.

Using this alternative formulation of $\overline{K}(q,t)$ we define ρ to be the shift map

$$\rho : \overline{K}(q,t) \to \overline{K}(q,t)$$

$$(\ldots, w_{i-1}, w_i, w_{i+1}, \ldots) \mapsto (\ldots, w_{i-2}, w_{i-1}, w_i, \ldots)$$

Lemma 3.5 *Shift map ρ is the unique map with the property that for all $k \geq 1$, its restriction to the subgroup isomorphic to $K(q,k,t)$, $\rho|_{K(q,k,t)}$, is ρ_k.*

Proof The subgroup of $\overline{K}(q,t)$ isomorphic to $K(q,k,t)$ is precisely the subgroup of vectors with period k. On a periodic vector, shifting is the same action as clockwise rotation on the truncated vector of length k. By the universal property of direct limits, there is a unique map which restricts to ρ_k for all $k \geq 1$, and thus that map is ρ. □

Furthermore, the following result is a consequence of our definition of ρ.

Theorem 3.6 *For all integers $k \geq 1$, $q \geq 0$ and $t \geq 1$, we have a group isomorphism*

$$K(q,k,t) \cong \operatorname{Ker}(1-\rho^k) : \overline{K}(q,t) \to \overline{K}(q,t).$$

In summary, if $|E(\mathbb{F}_q)| = N_1$ and we let $t = -N_1$, then we have correspondences between

$$\begin{array}{rcl} K(q,k,t) & \text{and} & E(\mathbb{F}_{q^k}), \\ \overline{K}(q,t) & \text{and} & E(\overline{\mathbb{F}_p}), \\ \text{Frobenius map } \pi & \text{and} & \text{Shift map } \rho \end{array}$$

with the property that $K(q,k_1,t) \leq K(q,k_2,t)$ if and only if $E(\mathbb{F}_{q^{k_1}}) \leq E(\mathbb{F}_{q^{k_2}})$, and $K(q,k,t) \leq \overline{K}(q,t)$ and $E(\mathbb{F}_{q^k}) \leq E(\overline{\mathbb{F}_p})$ for all integers $k \geq 1$.

4 Factorization of the polynomial $\mathcal{W}_k(Q,T)$

We now turn our attention to the problem of factoring the bivariate polynomials $\mathcal{W}_k(Q,T)$ into irreducibles over $\mathbb{Z}[Q,T]$. For the factorization, we use the cyclotomic polynomials, denoted by $\{Cyc_d(x)\}$, which are a family of integral irreducible polynomials defined uniquely by the property

$$1-x^k=\prod_{d|k} Cyc_d(x) \quad \text{for all } k\geq 1.$$

The cyclotomic polynomials have degree $\phi(d)$, which is the Euler function defined as the number of integers $e\in\{1,2,\dots,d-1\}$ such that d and e are relatively prime. As in the case of cyclotomic polynomials, we shall show that the irreducible factors of $\mathcal{W}_k(Q,T)$ are also parametrized by divisors of k.

Theorem 4.1 *There exists a unique family of bivariate irreducible integral polynomials indexed by positive integers, which we denote by $WCyc_d(Q,T)$, such that*

$$\mathcal{W}_k(Q,T)=\prod_{d|k} WCyc_d(Q,T)$$

for all $k\geq 1$. Further, $WCyc_d(Q,T)$ is of degree $\phi(d)$ in both Q and T.

Proof We use Proposition 12 of [12] which stated the existence of a family of bivariate irreducible integral polynomials, indexed by positive integers and denoted by $ECyc_d(Q,T)$ such that for all elliptic curves E, and all finite fields $\mathbb{F}_q$,

$$|E(\mathbb{F}_{q^k})|=\prod_{d|k} ECyc_d(Q,T)|_{Q=q,T=-N_1}.$$

Since $|E(\mathbb{F}_{q^k})|=-\mathcal{W}_k(Q,T)|_{Q=q,T=-N_1}$, it follows that

$$\mathcal{W}_k(Q,T)|_{Q=q,T=-N_1}=(-N_1)\prod_{\substack{d|k\\ d\neq 1}} ECyc_d(Q,T)|_{Q=q,T=-N_1}$$

for all elliptic curves E and prime powers q. Consequently, we have a polynomial identity

$$\mathcal{W}_k(Q,T)=T\prod_{\substack{d|k\\ d\neq 1}} ECyc_d(Q,-T).$$

We define $WCyc_1(Q,T)=T$ and $WCyc_d(Q,T)=ECyc_d(Q,-T)$ otherwise, and obtain the decomposition $\mathcal{W}_k(Q,T)=\prod_{d|k} WCyc_d(Q,T)$. The polynomials $WCyc_d(Q,T)$ have integer coefficients since this property was true of the polynomials $ECyc_d(Q,T)$. Furthermore, if any of the $WCyc_d(Q,T)$'s were reducible, then by applying the map $T\mapsto -T$, we would get a factorization of $ECyc_d(Q,T)$, thus we conclude that $WCyc_d(Q,T)$ are irreducible polynomials. Lastly, $WCyc_d(Q,T)$ has degree $\phi(d)$ in both Q and T since $ECyc_d(Q,T)$ had this property by Proposition 14 of [12]. □

A few of the first polynomials $WCyc_d(Q,T)$ are given below for small d's with no prime powers greater than 5:

$$\begin{aligned}
WCyc_1 &= T\\
WCyc_2 &= T + 2(1+Q)\\
WCyc_3 &= T^2 + (3+3Q)T + 3(1+Q+Q^2)\\
WCyc_4 &= T^2 + (2+2Q)T + 2(1+Q^2)\\
WCyc_5 &= T^4 + (5+5Q)T^3 + (10+15Q+10Q^2)T^2\\
&\quad + (10+15Q+15Q^2+10Q^3)T\\
&\quad + 5(1+Q+Q^2+Q^3+Q^4)\\
WCyc_6 &= T^2 + (1+Q)T + (1-Q+Q^2)\\
WCyc_8 &= T^4 + (4+4Q)T^3 + (6+8Q+6Q^2)T^2\\
&\quad + (4+4Q+4Q^2+4Q^3)T + 2(1+Q^4)\\
WCyc_9 &= T^6 + (6+6Q)T^5 + (15+24Q+15Q^2)T^4\\
&\quad + (21+36Q+36Q^2+21Q^3)T^3\\
&\quad + (18+27Q+27Q^2+27Q^3+18Q^4)T^2\\
&\quad + (9+9Q+9Q^2+9Q^3+9Q^4+9Q^5)T\\
&\quad + 3(1+Q^3+Q^6)\\
WCyc_{10} &= T^4 + (3+3Q)T^3 + (4+3Q+4Q^2)T^2 + (2+Q+Q^2+2Q^3)T\\
&\quad + (1-Q+Q^2-Q^3+Q^4)\\
WCyc_{12} &= T^4 + (4+4Q)T^3 + (5+8Q+5Q^2)T^2 + (2+2Q+2Q^2+2Q^3)T\\
&\quad + (1-Q^2+Q^4).
\end{aligned}$$

Using critical groups, we obtain a combinatorial definition of the evaluation $WCyc_d(q,t)$, which is a shorthand for $WCyc_d(Q,T)|_{Q=q,T=t}$. Recall that in Section 3, $\overline{K}(q,t)$ was defined to be the direct limit of $\{K(q,k,t)\}_{k=1}^{\infty}$, ρ was defined as the unique map with the universal property that for all $k \geq 1$, the restriction of ρ to $K(q,k,t)$ is ρ_k, and $Cyc_d(x)$ denotes the dth cyclotomic polyonomial. Since $\overline{K}(q,t)$ is abelian and ρ commutes with the addition of $\overline{K}(q,t)$, the expression $Cyc_d(\rho)$ defines a well-defined group homomorphism: $\overline{K}(q,t) \to \overline{K}(q,t)$.

Theorem 4.2 *For all integers $d \geq 1, q \geq 0, t \geq 1$, we have equality*

$$WCyc_d(q,t) = \left|\mathrm{Ker}\Big(Cyc_d(\rho)\Big) : \overline{K}(q,t) \to \overline{K}(q,t)\right|.$$

Remark 4.3 In [12], an analogous group theoretic interpretation was given for the polynomials $ECyc_d(q,t)$. We observe that since the cyclotomic polynomials have integer coefficients and the Frobenius map, π, is compatible with the group law on the elliptic curve, the expression $Cyc_d(\pi)$ defines a map, more precisely an isogeny, from an elliptic curve defined over $\mathbb{F}_q$ back to itself. Theorem 7 of [12] stated that for all $d \geq 1$,

$$ECyc_d(q, N_1) = \left|\text{Ker}\left(Cyc_d(\pi)\right) : E(\overline{\mathbb{F}_p}) \to E(\overline{\mathbb{F}_p})\right|$$

for all powers of prime q and all elliptic curves E defined over $\mathbb{F}_q$.

Proof The proof of Theorem 4.2 is analogous to the elliptic curve case. Since the maps $Cyc_{d_1}(\rho)$ and $Cyc_{d_2}(\rho)$ are group homomorphisms on $\overline{K}(q,t)$, we get

$$\left|\text{Ker}\left(Cyc_{d_1}(\rho)\ Cyc_{d_2}(\rho)\right)\right| = |\text{Ker}\, Cyc_{d_1}(\rho)| \cdot |\text{Ker}\, Cyc_{d_2}(\rho)|$$

and the rest of the proof follows as in [12]. □

Another comparison of shift map ρ and Frobenius map ρ is highlighted below.

Theorem 4.4 *As a map from $\overline{K}(q,t)$ to itself, we get*

$$\rho^2 - (1+q+t)\rho + q = 0.$$

Note that this quadratic equation is a simple analogue of the characteristic equation

$$\pi^2 - (1+q-N_1)\pi + q = 0$$

of the Frobenius map π. In the case of elliptic curves, this equation is proven by analyzing endomorphisms on the torsion points, via the Tate Module [14, pg. 135] or via the Weil Pairing [18, Theorem 4.10]. However in the critical group case, linear algebra suffices.

Proof of Theorem 4.4 By the universal property of ρ, it suffices to prove the identity on $K(q,k,t)$ for all $k \geq 1$. In particular, if $\rho(C) = [c_k, c_1, c_2, \ldots, c_{k-2}, c_{k-1}]^T$, then we notice that $\rho^2(C) - (1+q+t)\rho(C) + q \cdot C$ equals

$$c_1 \begin{bmatrix} q \\ -(1+q+t) \\ -1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 \\ q \\ -(1+q+t) \\ -1 \\ \vdots \\ 0 \\ 0 \end{bmatrix} + \cdots + c_k \begin{bmatrix} -(1+q+t) \\ -1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ q \end{bmatrix},$$

which equals $[0,0,0,0,\ldots,0,0]^T$ modulo the columns of the reduced Laplacian matrix. □

An even more surprising connection is the subject of the next section.

5 Group presentations

It is well known that an elliptic curve over a finite field has a group structure which is the product of at most two cyclic groups. See [14, pg. 145] or [18, Theorem 4.1] for an example. In view of the above results for elliptic curves, it is natural to wonder what is the group structure of $K(q,k,t)$.

The case of a simple wheel graph W_k was explicitly found in [2] to be

$$\mathbb{Z}/L_k\mathbb{Z}\times\mathbb{Z}/L_k\mathbb{Z} \quad\text{or}\quad \mathbb{Z}/F_{k-1}\mathbb{Z}\times\mathbb{Z}/5F_{k-1}\mathbb{Z}$$

depending on whether k is odd or even, respectively. Here L_k is the kth Lucas number and F_k is the kth Fibonacci number.

Determining such structures of critical groups has been the subject of several recent papers, e.g. [7, 10, 11], and a common tool is the Smith normal form of the Laplacian. In particular, if G is isomorphic to $\mathbb{Z}^m/\operatorname{Im} M$, and M' has the same Smith normal form as M, then G is also isomorphic to $\mathbb{Z}^m/\operatorname{Im} M'$. Matrices M and M' have the same Smith normal form if and only if M can be transformed into M' by the following three operations:

(1) Multiplication of a row or a column by -1.
(2) Addition of an integer multiple of a row or column to another.
(3) Swapping of two rows or two columns.

Theorem 5.1 *The abelian group $K(q,k,t)$ has a group structure that can be written as the product of at most two cyclic groups.*

Proof We let M_k be the k-by-k circulant matrix $circ(1+q-N_1,-q,0,\dots,0,-1)$ as in Section 1.1, and let $\overline{M}_k$ denote the k-by-k matrix $circ(1+q+t,-q,0,\dots,0,-1)$, the reduced Laplacian of the (q,t)-wheel graph. (For the case of $k=1$ or $k=2$, we get degenerate versions of M_k but since these matrices are one and two dimensional respectively, their Smith normal forms cannot contain diagonals with more than two nontrivial elements. Hence, for any $q\geq 0$ and $t\geq 1$, $K(q,1,t)$ and $K(q,2,t)$ satisfy the theorem.) We thus assume that $k\geq 3$. To begin we note that after permuting rows cyclically and multiplying all rows by (-1), we get

$$\overline{M}_k^T \equiv \begin{bmatrix} 1 & 0 & \dots & 0 & q & -1-q-t \\ -1-q-t & 1 & 0 & \dots & 0 & q \\ q & -1-q-t & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & 0 & q & -1-q-t & 1 & 0 \\ 0 & \dots & 0 & q & -1-q-t & 1 \end{bmatrix}.$$

Except for the upper-right corner of three nonzero entries, this matrix is lower-triangular with ones on the diagonal. Adding a multiple of the first row to the second and third rows, respectively, we obtain a new matrix with vector

$$[1,0,0,\dots,0]^T$$

as the first column. Since we can add multiples of columns to one another as well, we also obtain a matrix with vector $[1, 0, 0, \dots, 0]$ as the first row.

This new matrix will again be lower triangular with ones along the diagonal, except for nonzero entries in four spots in the last two columns of rows two and three. By symmetry and sparseness of this matrix, we can continue this process, which will always shift the nonzero block of four in the last two columns one row down. This process will terminate with a block diagonal matrix consisting of $(k-2)$ 1-by-1 blocks of element 1 followed by a single 2-by-2 block.

Thus, the Smith normal form of M_k is the same as the Smith normal form of a matrix formed by taking the direct sum of the identity matrix and a 2-by-2 block. The only way to calculate the exact Smith normal form of M_k is to use precise integers for q and t, however in our general manipulations we treated these as symbolic variables. Nonetheless, there will be at most two nontrivial entries on the diagonal of such a Smith normal form, thus we are done. □

Since this proof is constructive, as an application we arrive at a presentation of $K(q,k,t)$ as the cokernels of a 2-by-2 matrix whose entries have combinatorial interpretations. Let $e(S)$ be the number of even elements in the set S and $\hat{F}_{2k}(q,t)$ be a bivariate analogue of the Fibonacci numbers defined by

$$\hat{F}_{2k}(q,t) = \sum_{S\subseteq\{1,2,\dots,2k\}:S \text{ contains no two consecutive elements}} q^{e(S)}\, t^{k-\#S}.$$

Corollary 5.2 *For $k \geq 3$, the Smith normal form of $\overline{M}_k$ is equivalent to a direct sum of the identity matrix and*

$$\begin{bmatrix} q\hat{F}_{2k-4}+1 & q\hat{F}_{2k-2} \\ \hat{F}_{2k-2} & \hat{F}_{2k}-1 \end{bmatrix}.$$

Before giving the proof of Corollary 5.2, we show the following more general result. Define $\widetilde{M}_k$ as the following k-by-k matrix:

$$\widetilde{M}_k = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 & A & B \\ -\Delta & 1 & 0 & \dots & 0 & 0 & C & D \\ q & -\Delta & 1 & \dots & 0 & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & -\Delta & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & q & -\Delta & W & X \\ 0 & 0 & 0 & \dots & 0 & q & Y & Z \end{bmatrix}.$$

Proposition 5.3 *The Smith normal form of $\widetilde{M}_k$ is equivalent to*

$$\begin{bmatrix} 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & a & b \\ 0 & 0 & \dots & 0 & c & d \end{bmatrix}$$

where $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} \Delta & 1 \\ -q & 0 \end{bmatrix}^{k-2} \begin{bmatrix} A & B \\ C & D \end{bmatrix} + \begin{bmatrix} W & X \\ Y & Z \end{bmatrix}$.

Proof We represent the last two columns of $\widetilde{M}_k$ as $\begin{bmatrix} a''_1 & b''_1 \\ a'_2 & b'_2 \\ a_3 & b_3 \\ a_4 & b_4 \\ a_5 & b_5 \\ \vdots & \vdots \\ a_k & b_k \end{bmatrix}$, and let $\begin{bmatrix} 0 & 0 \\ a''_2 & b''_2 \\ a'_3 & b'_3 \\ a_4 & b_4 \\ a_5 & b_5 \\ \vdots & \vdots \\ a_k & b_k \end{bmatrix}$ signify the last two columns after completing the steps outlined above, i.e. subtracting a multiple of the first row from the second and third rows, and then using the first column to cancel out the entries a''_1 and b''_1.

Continuing inductively, we get the relations

$$\begin{aligned} a''_m &= \Delta a''_{m-1} + a'_m \\ b''_m &= \Delta b''_{m-1} + b'_m \\ a'_{m+1} &= q a''_{m-1} + a_{m+1} \\ b'_{m+1} &= q b''_{m-1} + b_{m+1}, \end{aligned}$$

which we encode as the matrix equation

$$\begin{bmatrix} a''_m & b''_m \\ a'_{m+1} & b'_{m+1} \end{bmatrix} = \begin{bmatrix} \Delta & 1 \\ -q & 0 \end{bmatrix} \begin{bmatrix} a''_{m-1} & b''_{m-1} \\ a'_m & b'_m \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ a_{m+1} & b_{m+1} \end{bmatrix}.$$

Letting $a_3, b_3, \dots, a_{k-2}, b_{k-2} = 0$ and using $\begin{bmatrix} \Delta & 1 \\ -q & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ W & X \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ Y & Z \end{bmatrix} = \begin{bmatrix} W & X \\ Y & Z \end{bmatrix}$, we obtain the desired result. □

We now wish to consider the special case $\Delta = 1 + q + t$, $\begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} q & -\Delta \\ 0 & q \end{bmatrix}$, and $\begin{bmatrix} W & X \\ Y & Z \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -\Delta & 1 \end{bmatrix}$. To simplify our expression further, we utilize the following formula for a specific sequence of matrix powers.

Lemma 5.4 *For all $m \geq 2$,*

$$\begin{bmatrix} 1+q+t & 1 \\ -q & 0 \end{bmatrix}^m = \begin{bmatrix} \hat{F}_{2m} & \hat{F}_{2m-2} \\ -q\hat{F}_{2m-2} & -q\hat{F}_{2m-4} \end{bmatrix}.$$

Proof We verify the result for $m = 2$ using the fact that

$$\begin{aligned} \hat{F}_0 &= 1 \\ \hat{F}_2 &= t + (1+q) \\ \hat{F}_4 &= t^2 + (2+2q)t + (1+q+q^2) = (1+q+t)^2 - q. \end{aligned}$$

The product $\begin{bmatrix} 1+q+t & 1 \\ -q & 0 \end{bmatrix} \begin{bmatrix} \hat{F}_{2m} & \hat{F}_{2m-2} \\ -q\hat{F}_{2m-2} & -q\hat{F}_{2m-4} \end{bmatrix}$ equals

$$\begin{bmatrix} (1+q+t)\hat{F}_{2m} - q\hat{F}_{2m-2} & (1+q+t)\hat{F}_{2m-2} - q\hat{F}_{2m-4} \\ \\ -q\hat{F}_{2m} & -q\hat{F}_{2m-2} \end{bmatrix}.$$

Thus it suffices to demonstrate

$$\hat{F}_{2m+4} = (1+q+t)\hat{F}_{2m+2} - q\hat{F}_{2m}$$

by recursion. This recurrence was proven in [12]; the proof is a generalization of the well-known recurrence $F_{2m+4} = 3F_{2m+2} - F_{2m}$ for the Fibonacci numbers.

Namely, the polynomial $\hat{F}_{2m+4}$ is a (q,t)-enumeration of the number of chains of $2m+4$ beads, with each bead being either black or white, and no two consecutive beads being both black. Similarly $(1+q+t)\hat{F}_{2m+2}$ enumerates the concatenation of such a chain of length $2m+2$ with a chain of length 2. One can recover a legal chain of length $2m+4$ this way except in the case where the $(2m+2)$nd and $(2m+3)$rd beads are both black. Since this forces the $(2m+1)$st and $(2m+4)$th beads to be white, such cases are enumerated by $q\hat{F}_{2m}$ and this completes the proof. With this recurrence, Lemma 5.4 is proven. □

Proof of Corollary 5.2 Here we give an explicit derivation of matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in terms of $\hat{F}_k(q,t)$. By Proposition 5.3 and Lemma 5.4, we let $m = k-2$ and we obtain

$$\begin{aligned} \begin{bmatrix} a & b \\ c & d \end{bmatrix} &= \begin{bmatrix} \hat{F}_{2k-4} & \hat{F}_{2k-6} \\ -q\hat{F}_{2k-6} & -q\hat{F}_{2k-8} \end{bmatrix} \begin{bmatrix} q & -1-q-t \\ 0 & q \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ -1-q-t & 1 \end{bmatrix} \\ &= \begin{bmatrix} q\hat{F}_{2k-4} + 1 & -(1+q+t)\hat{F}_{2k-4} + q\hat{F}_{2k-6} \\ -q^2\hat{F}_{2k-6} - 1 - q - t & (1+q+t)q\hat{F}_{2k-6} - q^2\hat{F}_{2k-8} + 1 \end{bmatrix} \end{aligned}$$

when reducing $\overline{M_k}^T$ to a 2-by-2 matrix with an equivalent Smith normal form.

We apply the recursion $\hat{F}_{2m+4} = (1+q+t)\hat{F}_{2m+2} - q\hat{F}_{2m}$ followed by adding a multiple of $(1+q+t)$ times the first row to the second row, and then use the recursion again to get $\begin{bmatrix} q\hat{F}_{2k-4}+1 & -\hat{F}_{2k-2} \\ q\hat{F}_{2k-2} & -\hat{F}_{2k}+1 \end{bmatrix}$. Finally we multiply the second row and column by (-1) and take the transpose, thereby obtaining the desired result. □

As stated in the introduction, q and t signify specific integers, so one can reduce the Smith normal form further. In general, the Smith normal form of a 2-by-2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ can be written as $\mathrm{diag}(d_1, d_1 d_2)$ where $d_1 = \gcd(a, b, c, d)$. The group $K(q, k, t)$ is cyclic if and only if $d_1 = 1$ in this case.

Question 5.5 How can one predict what choices of integers (k, q, t) lead to a cyclic critical group, and can we more precisely describe the group structure otherwise?

Answering this question for $W_k(q, t)$ is difficult since the Smith normal form of even a 2-by-2 matrix can vary wildly as the four entries change, altering the greatest common divisor along with them. However, we give a partial answer to this question below, after considering a related family of graphs.

Remark 5.6 In [3], Biggs shows that a family of deformed wheel graphs (with an odd number of vertices) have cyclic critical groups. We are able to obtain a generalization of this result here by using Proposition 5.3. The author thanks Norman Biggs [4] for bringing this family of graphs to the author's attention.

Biggs defined $\widetilde{W_k}$ by taking the simple wheel graph W_k with k rim vertices and adding an extra vertex on one of the rim vertices. Equivalently, $\widetilde{W_k}$ can be constructed from W_{k+1} by removing one spoke. We construct a (q, t)-deformation of this family by defining $\widetilde{W_k(q, t)}$ as the graph $W_{k+1}(q, t)$ where all edges, i.e. spokes, connecting vertex v_0 and v_1 are removed.

With such a deformation, it is no longer true that this entire family of graphs has cyclic critical groups, but the next theorem gives a precise criterion for cyclicity and further gives an explicit formula for the smaller of the two invariant factors otherwise. Let $[k+1]_q = 1 + q + q^2 + \cdots + q^k$ be the usual q-analogue of $(k+1)$.

Theorem 5.7 *If integers $q \geq 0$ $k \geq 1$, $t \geq 1$ satisfy $\gcd(t, [k+1]_q) = 1$ then the critical group of $\widetilde{W_k(q, t)}$ is cyclic. Otherwise, if we let $d_1 = \gcd(t, [k+1]_q)$, then $\widetilde{W_k(q, t)} \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_1 d_2\mathbb{Z}$.*

Proof Notice, that the reduced Laplacian matrix for $\widetilde{W_k(q, t)}$ agrees with the matrix $\overline{M}_{k+1}$ except in the first entry corresponding to the outdegree of v_1. After taking the transpose, cyclically permuting the rows, and multiplying by (-1), we obtain a matrix adhering to the hypothesis of Proposition 5.3 with $\begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} q & -1-q \\ 0 & q \end{bmatrix}$ and

$\begin{bmatrix} W & X \\ Y & Z \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1-q+N_1 & 1 \end{bmatrix}$. Thus, the 2-by-2 matrix for this case equals

$$\begin{bmatrix} \hat{F}_{2k-2} & \hat{F}_{2k-4} \\ -q\hat{F}_{2k-4} & -q\hat{F}_{2k-6} \end{bmatrix} \begin{bmatrix} q & -1-q \\ 0 & q \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ -1-q-t & 1 \end{bmatrix}$$
$$= \begin{bmatrix} q\hat{F}_{2k-2}+1 & -(1+q)\hat{F}_{2k-2}+q\hat{F}_{2k-4} \\ -q\hat{F}_{2k-4}-1-q-t & (1+q)q\hat{F}_{2k-4}-q^2\hat{F}_{2k-6}+1 \end{bmatrix}.$$

As in Corollary 5.2, we add $(1+q+t)$ times the first row to the second row, and then multiply the second column by (-1) to arrive at

$$\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} q\hat{F}_{2k-2}+1 & (1+q)\hat{F}_{2k-2}-q\hat{F}_{2k-4} \\ q\hat{F}_{2k} & (1+q)\hat{F}_{2k}-q^2\hat{F}_{2k-2}+1 \end{bmatrix}$$
$$= \begin{bmatrix} q\hat{F}_{2k-2}+1 & \hat{F}_{2k}-t\hat{F}_{2k-2} \\ q\hat{F}_{2k} & \hat{F}_{2k+2}-t\hat{F}_{2k}-1 \end{bmatrix}.$$

We can reduce this by plugging in specific values for q and t and checking whether or not $[k+1]_q = 1+q+\cdots+q^k$ and t share a common factor. We know that there exist unique d_1 and d_2 such that $\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ is Smith equivalent to $\begin{bmatrix} d_1 & 0 \\ 0 & d_1 d_2 \end{bmatrix}$. We begin by showing that d_1 must divide t.

Suppose otherwise; then there exists a prime p and a positive integer ℓ such that p^ℓ divides d_1 but p^ℓ does not divide t. Looking at the off-diagonal entries b' and c', we see that d_1 divides $q\hat{F}_{2k}$ and $\hat{F}_{2k}-t\hat{F}_{2k-2}$ hence p^ℓ divides both of them. Dividing the three quantities $q\hat{F}_{2k}$, $\hat{F}_{2k}-t\hat{F}_{2k-2}$, and t by the largest power of p which divides t, we may assume without loss of generality that $p|q\hat{F}_{2k}$, $p|(\hat{F}_{2k}-t\hat{F}_{2k-2})$, but $p\nmid t$. Since p does not divide t, p must divide either q or $\hat{F}_{2k-2}$. However, d_1, and hence p, must also divide the top left entry, which is $q\hat{F}_{2k-2}+1$. Thus we get a contradiction, and conclude that $d_1|t$.

This greatly limits the possibilities for d_1. Furthermore, if we work modulo t, the equivalence class of a', b', c', and d' (modulo d_1) does not change.

Letting $t=0$ in $\hat{F}_{2k}$ is equivalent to counting subsets of $\{1,2,\ldots,2k\}$ of size k with no two elements consecutive. We can choose the subsets of all odd numbers, which will have weight 1. If we then pick element $2k$ instead of $2k-1$, we get a subset of weight q, and inductively, we get a weighted sum of $1+q+q^2+\cdots+q^k$ where the last weight corresponds to the subset of all even numbers. Thus the desired 2-by-2 matrix reduces to $\begin{bmatrix} q(1+q+q^2+\cdots+q^{k-1})+1 & 1+q+q^2+\cdots+q^k \\ q(1+q+q^2+\cdots+q^k) & q+q^2+\cdots+q^{k+1} \end{bmatrix}$, hence modulo t, the gcd of the entries is the quantity $[k+1]_q$.

Thus we conclude that d_1 divides $[k+1]_q$. Combining this fact with $d_1|t$, we conclude that $d_1|\gcd([k+1]_q, t)$. However, since we know that $d_1 \equiv [k+1]_q \pmod{t}$, we have integers m_1, m_2 such that $t = m_1 d_1$, $[k+1]_q = (m_1 m_2 + 1)d_1$, and so $\gcd([k+1]_q, t) = d_1 \cdot m_3$ where $m_3 = \gcd(m_1, m_1 m_2 + 1) = 1$. Thus we obtain the equality $d_1 = \gcd([k+1]_q, t)$ as desired. □

Remark 5.8 Notice, that if $q = 1$ and $t = 1$ we have $d_1 = 1$, hence we have cyclicity in this case. This result was proven by Biggs [3] for the case of odd k, and the above proof of Theorem 5.7 specializes to give an alternate proof of this result.

Remark 5.9 The above proof can also be adapted to demonstrate the values of (k, q, t) for which the original critical groups, $K(q, k, t)$, are not cyclic. Namely, by pushing through the same argument, we find that modulo t, the value d_1 is congruent to $[k]_q$. Consequently, the quantity $\gcd(t, [k]_q)$ divides the gcd of a, b, c, d, and thus $K(q, k, t)$ is *not* cyclic whenever $K(\widetilde{W_{k-1}}(q, t))$ is *not* cyclic. Unfortunately, we do not get an if and only if criterion nor a precise formula for the smaller invariant factor in this case. This is due to the fact that there are cases where d_1 does not divide t for the undeformed wheel graphs. In particular, this allows the simple wheel graphs to have non-cyclic critical groups.

Despite the fact that it is difficult to determine whether or not $K(q, k, t)$ is cyclic, if we instead look at the limit, $\overline{K}(q, t)$, we have the following result:

Theorem 5.10 *For any $n \geq 1$, the abelian group $\overline{K}(q, t)$ contains the subgroup $\mathbb{Z}/n\mathbb{Z}$. Furthermore, $\overline{K}(q, t)$ contains $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as a subgroup if and only if n and q are coprime.*

For the proof of Theorem 5.10, we will utilize the following lemma, which is a variant of a result of D. D. Wall [17].

Lemma 5.11 *Let $\{\hat{G}_m(Q, T)\}_{m\geq 1}$ be any sequence of bivariate integer polynomials satisfying the recurrence*

$$\hat{G}_{m+2} = (1 + Q + T)\hat{G}_{m+1} - Q\hat{G}_m.$$

If q, t, n are integers, $n \geq 1$, then the sequence $\{\hat{G}_m(Q, T)|_{Q=q,T=t} \mod n\}_{m\geq 1}$ is periodic.

Proof Given integers q, t, let $\hat{G}_m$ be shorthand for $\hat{G}_m(Q, T)|_{Q=q,T=t}$. Since there a a finite number of choices of pairs, n^2, and an infinite number of m, there clearly exist $m, m' \geq 1$ such that we have both

$$\hat{G}_m \equiv \hat{G}_{m'} \mod n \text{ and}$$
$$\hat{G}_{m+1} \equiv \hat{G}_{m'+1} \mod n.$$

Since $\hat{G}_{m+2} = (1+q+t)\hat{G}_{m+1} - q\hat{G}_m$, we use this modular equivalence and induction to prove that $\hat{G}_{m+r} \equiv \hat{G}_{m'+r} \mod n$ for all $r \geq 0$. Running the recurrence backwards, we see that this equivalence is also true for $\hat{G}_{m-1} \equiv \hat{G}_{m'-1}$, $\hat{G}_{m-2} \equiv \hat{G}_{m'-2}$, $\ldots$, $\hat{G}_1 \equiv \hat{G}_{(m'-m)+1}$, $\hat{G}_0 \equiv \hat{G}_{m'-m}$ and we have the desired periodicity. □

Proof of Theorem 5.10 Because $\overline{K}(q, t)$ is the direct limit of abelian groups $K(q, k, t)$ using injective transition maps, it follows that $K(q, k, t)$ is isomorphic to a subgroup of $\overline{K}(q,t)$ for all $k \geq 1$. Thus, any group G is a subgroup of $\overline{K}(q,t)$ if and only if there exists k such that G is a subgroup of $K(q,k,t)$. (In fact, once $G \leq K(q,k,t)$, we have $G \leq K(q,mk,t)$ for all $m \geq 1$.)

By Theorems 2 and 3 of [12], it follows that $\mathcal{W}_k(Q,T) = \hat{L}_{2k}(Q,T) - (1+Q^k)$, where

$$\hat{L}_{2k} = \sum_{S \subseteq \{1,2,\ldots,2k\}\ :\ S \text{ contains no two } \textit{circularly} \text{ consecutive elements}} Q^{e(S)}\ T^{k-\#S}$$

is a bivariate analogue of the Lucas number L_{2k}. These bivariate analogues of the Lucas numbers actually satisfy the recurrence [12, Proposition 1]

$$L_{2k+4} = (1+Q+T)L_{2k+2} - QL_{2k},$$

so the hypotheses of Lemma 5.11 are satisfied. We conclude that for all integers q and t, the sequence of integers $\{\hat{L}_{2k}(q,t) \mod n\}_{k\geq 1}$ is periodic. By Fermat's Little Theorem, $q^{\phi(n)} \equiv 1 \mod n$ so $\{1+q^k \mod n\}_{k\geq 1}$ is also periodic, and thus their sum $\{\mathcal{W}_k(q,t) \mod n\}_{k\geq 1}$ is a periodic sequence. Assuming that the period of $\{\mathcal{W}_k(q,t) \mod n\}_{k\geq 1}$ is k_0, it follows that

$$\mathcal{W}_{k_0+1}(q,t) \equiv \mathcal{W}_1(q,t) \equiv (1+q+t) - (1+q^1) \text{ and}$$
$$\mathcal{W}_{k_0+2}(q,t) \equiv \mathcal{W}_2(q,t) \equiv \Big((1+q+t)^2 - 2q\Big) - (1+q^2).$$

By the recurrence for the $\hat{L}_{2k}$'s, $\mathcal{W}_{k_0} \equiv \hat{L}_{2k_0} - (1+q^0) \equiv 2-2 \equiv 0$. Consequently, n divides $\mathcal{W}_{k_0}(q,t)$, and since this is the order of $K(q,k_0,t)$, a finite abelian group, when $q \geq 0$ and $t \geq 1$, it follows that $K(q,k_0,t)$ contains a subgroup of order n. Thus for all $q \geq 0$, $t \geq 1$, $n \geq 1$, the limit $\overline{K}(q,t)$ contains a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

We now turn to the question of whether or not $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is a subgroup of $\overline{K}(q,t)$. From Corollary 5.2, we see that for $k \geq 3$, the Smith normal form of $\overline{M}_k^T$ is equivalent to a direct sum of the identity matrix and $\begin{bmatrix} q\hat{F}_{2k-4}+1 & q\hat{F}_{2k-2} \\ \hat{F}_{2k-2} & \hat{F}_{2k}-1 \end{bmatrix}$. Thus

$$\mathbb{Z}^k / \operatorname{Im} \overline{M}_k^T \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$$

where $d_1 | d_2$ and $d_1 = \gcd(q\hat{F}_{2k-4}+1, q\hat{F}_{2k-2}, \hat{F}_{2k-2}, \hat{F}_{2k}-1)$. Using the fact that $\hat{F}_{2k} - 1 = (1+q+t)\hat{F}_{2k-2} - (q\hat{F}_{2k+4}+1)$, we can simplify this gcd to

$$d_1 = \gcd(q\hat{F}_{2k-4}+1, \hat{F}_{2k-2}).$$

Let k_0 denote the period of the sequence $\{\hat{F}_{2k}(q,t) \mod n\}_{k\geq 1}$. Accordingly, of $\hat{F}_{2k_0} \equiv 1 \mod n$ and $\hat{F}_{2k_0+2} \equiv (1+q+t) \mod n$. If q and n are coprime, we can run the $\hat{F}_{2k}$-recurrence backwards, to see that $\hat{F}_{2k_0-2} \equiv 0 \mod n$ and $\hat{F}_{2k_0-4} = 0 \equiv -1/q \mod n$. Notice that $\gcd(\hat{F}_{2k_0-2}, q\hat{F}_{2k_0-4} - 1) \equiv (0,0)$ modulo n and we conclude that n divides d_1, the gcd associated to the 2-by-2 matrix for $\overline{M}_{k_0}$. Thus we see that $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \leq \overline{K}(q,t)$ when q and n are coprime.

If q and n share a common factor, then $d_1 = \gcd(q\hat{F}_{2k-4}+1, \hat{F}_{2k-2}) \not\equiv 0$ modulo n for any k, since $q\hat{F}_{2k-4}+1 \equiv 1 \mod \gcd(q,n)$. Thus $(q,n) \neq 1$ implies that $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \not\leq \overline{K}(q,t)$. □

Remark 5.12 When q is a power of a prime (i.e. $q = p^\ell$), E is an elliptic curve, and $\overline{\mathbb{F}_p}$ is an algebraic closure of $\mathbb{F}_q$, the group of points $E(\overline{\mathbb{F}_p})$ also has the property that $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \leq E(\overline{\mathbb{F}_p})$ iff (n,q) coprime. When E is an ordinary elliptic curve, $\mathbb{Z}/p\mathbb{Z} \leq E(\overline{\mathbb{F}_p})$ and otherwise E is known as supersingular.

Thus Theorem 5.10 illustrates how $\overline{K}(q,t)$ behaves like an *ordinary* elliptic curve rather than a supersingular one. As we will see in Theorem 5.13, we should in fact think of $\overline{K}(q,t)$ as the combinatorial analogue of an even more specific type of ordinary elliptic curve, namely one with the endomorphism ring given by $\mathbb{Z}[\pi]$.

We now use analogous techniques to partially provide an explicit presentation for $E(\mathbb{F}_{q^k})$, the group of points/$\mathbb{F}_{q^k}$ on elliptic curve E, defined over $\mathbb{F}_q$. Recall that matrix M_k was defined in Section 2.

Theorem 5.13 *Let E be an elliptic curve defined over $\mathbb{F}_q$. If $End(E) \cong \mathbb{Z}[\pi]$, then*

$$E(\mathbb{F}_q^k) \cong \mathbb{Z}^k / \operatorname{Im} M_k^T$$

for all $k \geq 1$. Furthermore, there exists a point $P \in E(\mathbb{F}_{q^k})$ with property $\pi^m(P) \neq P$ for all $1 < m < k$ such that $\{P, \pi(P), \dots, \pi^{k-1}(P)\}$ are the set of generators of group $E(\mathbb{F}_{q^k})$ under this presentation.

Proof Since π satisfies a quadratic characteristic equation, the fact that $\mathrm{End}(E) \cong \mathbb{Z}[\pi]$ implies that we are in the case of an *ordinary* elliptic curve [18, Theorem 10.7]. In this case, all of E's endomorphisms are defined over $\mathbb{F}_q$, and more precisely, a theorem of Lenstra [8] says that an *ordinary* elliptic curve over $\mathbb{F}_q$ has a group structure in terms of its endomorphism ring, namely,

$$E(\mathbb{F}_{q^k}) \cong \mathrm{End}(E)/(\pi^k - 1).$$

Since $E(\mathbb{F}_{q^k}) \cong \mathbb{Z}[\pi]/(1-\pi^k)$, from the characteristic equation for the Frobenius map π, we get

$$E(\mathbb{F}_{q^k}) \cong \mathbb{Z}[x]/(x^2 - (1+q-N_1)x + q, \;\; x^k - 1)$$

with x transcendent over $\mathbb{Q}$. Thus $E(\mathbb{F}_{q^k})$ is isomorphic to a group with generators $\{1, x, x^2, \dots, x^{k-1}\}$ and relations generated by $\{x^2 - (1+q-N_1)x + q,\; x^3 - (1+q-N_1)x^2 + qx,\; \dots,\; x^{k-1} - (1+q-N_1)x^{k-2} + qx^{k-3},\; 1 - (1+q-N_1)x^{k-1} + qx^{k-2},\; x - (1+q-N_1) + qx^{k-1}\}$, hence matrix M_k, as defined in Section 1.1, is the desired presentation for $E(\mathbb{F}_{q^k})$. Letting x be π and acting on a point P, with the property $\pi^\ell(P) \neq P$ for $1 \leq \ell \leq k-1$, yields the desired generators. □

Note that we get that $\mathrm{End}(E) \cong \mathbb{Z}[\pi]$ implies that $E(\mathbb{F}_q)$ is cyclic, thus agreeing with the group presentation in the case when M_k^T is a 1-by-1 matrix. Since $E(\overline{\mathbb{F}_p})$ is the direct limit of $\{E(\mathbb{F}_{q^k})\}_{k\geq 1}$, we get the following corollary, following reasoning analogous to that of Section 3.

Corollary 5.14 *If* $\mathrm{End}(E) \cong \mathbb{Z}[\pi]$, *then* $E(\overline{\mathbb{F}_p})$ *is isomorphic to the direct limit of* $\{\ \mathbb{Z}^k/\mathrm{Im}\ M_k^T\ \}_{k\geq 1}$ *using the transition maps* ψ_{k_2,k_1} *defined in Section* 3.

Remark 5.15 C. Wittmann [19] describes in more generality how the groups $E(\mathbb{F}q^k)$ depend on $\mathrm{End}(E)$. He gives a description of $E(\mathbb{F}_{q^k})$ as a product of two cyclic groups, rather than as a cokernel of a $k-$by$-k$ matrix.

We leave the reader with two motivational questions for future research.

Question 5.16 If E is an elliptic curve defined over $\mathbb{F}_q$ and $\mathrm{End}(E) \neq \mathbb{Z}[\pi]$, can we state an analogue of Corollary 5.14? In other words, is there a sequence of integers $\{d(\ell)\}$ and another family of matrices $\hat{M}_\ell$, which analogously to the M_k^T have symmetries or are defined by a small number of parameters, such that $E(\overline{\mathbb{F}_p}) \cong$ the direct limit $\{\ \mathbb{Z}^{d(\ell)}/\ \mathrm{Im}\ \hat{M}_\ell\}_{\ell\geq 1}$ in this case?

Question 5.17 Even more generally, are there other families of curves $\mathcal{F}$ and other families of graphs $\mathcal{G}$ such that the Jacobian groups of $\mathcal{F}$ correspond to the critical groups of $\mathcal{G}$?

Acknowledgements This work first appeared in the author's Ph.D. Thesis at the University of California, San Diego, alongside the article "Combinatorial Aspects of Elliptic Curves" [12]. The author enthusiastically thanks his advisor Adriano Garsia for his guidance and many useful conversations. Conversations with Tewodros Amdeberhan, Norman Biggs, Dino Lorenzini, Richard Stanley, and Nolan Wallach have also been very helpful, and the referees' comments have helped to improve this exposition. The author would like to thank the NSF and the ARCS Foundation for their support during the author's graduate school. A preprint of the present article was presented at FPSAC 2007 in Tianjin, China.

References

1. Baker, M., Norine, S.: Riemann-Roch and Abel-Jacobi Theory on a Finite Graph. Adv. Math. **215**, 766–788 (2007)
2. Biggs, N.L.: Chip-firing and the critical group of a graph. J. Algebr. Comb. **9**, 22–45 (1999)
3. Biggs, N.L.: The critical group from a cryptographic perspective. Bull. London Math. Soc. (2007). 8 pages
4. Biggs, N.L.: Personal Communication
5. Dhar, D.: Self-organized critical state of sandpile automaton models. Phys. Rev. Lett. **64**(14), 1613–1616 (1990)
6. Gabrielov, A.: Abelian avalanches and Tutte polynomials. Physica A **195**, 253–274 (1993)
7. Jacobson, B., Neidermaier, A., Reiner, V.: Critical groups for complete multipartite graphs and Cartesian products of complete graphs (2002). http://www.math.umn.edu/~reiner/Papers/papers.html
8. Lenstra, H.W.: Complex multiplication structure of elliptic curves. J. Number Theory **56**, 227–241 (1996)
9. Lorenzini, D.: On a finite group associated to the Laplacian of a graph. Discr. Math. **91**, 277–282 (1991)
10. Lorenzini, D.: Smith normal form and Laplacians (2007). http://www.math.uga.edu/~lorenz/paper.html
11. Maxwell, M.: Enumerating bases of self-dual matroids (2006). http://garsia/math.yorku.ca/fpsac06/papers73.pdf

12. Musiker, G.: Combinatorial aspects of elliptic curves. Seminaire Lotharingien de Combinatoire **56** (2007), Article B56f
13. Postnikov, A., Shapiro, B.: Trees, parking functions, syzygies, and deformations of monomial ideals. Trans. Amer. Math. Soc. **356**(8), 3109–3142 (2004)
14. Silverman, J.: The arithmetic of elliptic curves. Graduate Texts in Mathematics, vol. 106. Springer-Verlag, New York (1986)
15. Stanley, R.P.: Enumerative combinatorics. Cambridge Studies in Advanced Mathematics, vol. 62. Cambridge University Press, Cambridge (1999)
16. Wagner, D.G.: The critical group of a directed graph (2000). arXiv:math.CO/0010241
17. Wall, D.D.: Fibonacci series modulo m. Amer. Math. Monthly **67**, 525–532 (1960)
18. Washington, L.: Elliptic curves: Number theory and cryptography. Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton (2003)
19. Wittmann, C.: Group structure of elliptic curves over finite fields. J. of Number Theory **88**, 335–344 (2001)