Claremont Colleges
Scholarship @ Claremont

HMC Senior Theses

HMC Student Scholarship

2015

A Combinatorial Exploration of Elliptic Curves

Matthew Lam
Harvey Mudd College

A Combinatorial Exploration of Elliptic Curves

Matt Lam

Nicholas J. Pippenger, Advisor

Michael R. Orrison, Reader

HARVEY
MUDD
COLLEGE

Department of Mathematics

May, 2015

Abstract

At the intersection of algebraic geometry, number theory, and combinatorics, an interesting problem is counting points on an algebraic curve over a finite field. When specialized to the case of elliptic curves, this question leads to a surprising connection with a particular family of graphs. In this document, we present some of the underlying theory and then summarize recent results concerning the aforementioned relationship between elliptic curves and graphs. A few results are additionally further elucidated by theory that was omitted in their original presentation.

Contents

Chapter 1

Background

1.1 Symmetric Functions

Our approach to the enumeration of points on curves is closely tied to the theory of symmetric functions. We therefore develop a bit of this theory so that we can discuss the enumeration of points in a naturally suited language.

Definition 1.1. *A homogeneous symmetric function of degree n is a formal power series*

$$f(x) = \sum_{\alpha} c_\alpha x^\alpha$$

where $\alpha = (\alpha_1, \alpha_2, \ldots)$ runs over all sequences of nonnegative integers whose sum is n, c_α is a scalar, and x^α represents the monomial $x_1^{\alpha_1} x_2^{\alpha_2} \cdots$. Furthermore, $f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots) = f(x_1, x_2, \ldots)$ for every permutation σ of the positive integers.

It is important to note that, despite their name, symmetric functions should be regarded as purely formal power series and not as actual functions to be evaluated. The set of all homogeneous symmetric functions of degree n is denoted by Λ^n, and the direct sum $\Lambda = \Lambda^0 \oplus \Lambda^1 \oplus \cdots$ is called the *algebra of symmetric functions*. We now describe three important generators of Λ and their relation to one another.

Definition 1.2. *For each positive integer k, we define the elementary symmetric function*

$$e_k = \sum_{i_1 < \cdots < i_k} x_{i_1} \cdots x_{i_k}\ , \quad k \geq 1 \quad (\textit{with } e_0 = 1).$$

In words, e_k is the sum of all distinct products of k distinct variables.

Definition 1.3. *For each positive integer k, we define the complete symmetric function*

$$h_k = \sum_{i_1 \le \cdots \le i_k} x_{i_1} \cdots x_{i_k}\ , \quad k \ge 1 \quad (\text{with } h_0 = 1).$$

In words, h_k is the sum of all distinct products of k not-necessarily distinct variables.

In both types of symmetric functions, the number of actual variables has not been specified. Also note the similarity between the two formal definitions; their relationship is quite analogous to the reciprocity between choose and multi-choose. In fact, taking the two symmetric functions in n variables and evaluating at $x_1 = \cdots = x_n = 1$, we obtain

$$\begin{aligned} e_k(1,\ldots,1) &= \sum_{i_1<\cdots<i_k} 1 = \binom{n}{k} \\ h_k(1,\ldots,1) &= \sum_{i_1\le\cdots\le i_k} 1 = \left(\!\!\binom{n}{k}\!\!\right) = (-1)^k\binom{-n}{k}. \end{aligned}$$

We expand upon this a bit further.

Proposition 1.1. *Define the endomorphism $\omega : \Lambda \to \Lambda$ by $\omega(e_n) = h_n$ [1]. Then ω is an involution, i.e. ω^2 is the identity automorphism.*

Proof. Define the auxiliary power series

$$E(t) = \sum_{n\ge 0} e_n t^n, \quad H(t) = \sum_{n \ge 0} h_n t^n.$$

Since the e_n contain products of distinct variables, and the h_n products of not-necessarily distinct variables, we can rewrite these series as

$$E(t) = \prod_i (1 + x_i t), \quad H(t) = \prod_i \frac{1}{1 - x_i t}.$$

For $H(t)$ we have used the closed form expression for a geometric series. It is then clear that $E(t)H(-t) = 1$, hence we can equate coefficients and apply ω to obtain

$$0 = \sum_{k=0}^{n} (-1)^{n-k} h_k \omega(h_{n-k}) = (-1)^n \sum_{k=0}^{n} (-1)^{n-k} \omega(h_k) h_{n-k}.$$

[1] The elementary symmetric functions generate Λ as an algebra, so this does in fact fully define an endomorphism. (For a proof of this, see Stanley (2001).)

The last step involved reindexing the summation $k \to n-k$, i.e. reversing the summation limits. Now consider $n=0$; it follows that $\omega(h_0)=1=e_0$. Consequently, by equating further coefficients the result follows inductively. □

This result generalizes the special case $\binom{n}{k} \to (-1)^k\binom{-n}{k}$ corresponding to $e_k(1,\ldots,1) \to h_k(1,\ldots,1)$ seen above. We now introduce one more class of symmetric functions.

Definition 1.4. *For each positive integer k, we define the power sum symmetric function*

$$p_k = \sum_i x_i^k\,, \quad k \geq 1 \quad (\textit{with } p_0 = 1).$$

Like the homogeneous and elementary symmetric functions, the power sum symmetric functions also generate Λ. However, it is often convenient to work with a linear basis for Λ. This brings us to the following proposition.

Proposition 1.2. *Recall that a partition λ of a positive integer n is a positive sequence $(\lambda_1,\ldots,\lambda_k)$ where $\sum_i \lambda_i = n$. Let $Par := \bigcup_{n\geq 0} Par(n)$, i.e. the set of all partitions of all positive integers. Then*

$$\{h_\lambda = h_{\lambda_1}\cdots h_{\lambda_k}\},\ \{e_\lambda = e_{\lambda_1}\cdots e_{\lambda_k}\},\ \{p_\lambda = p_{\lambda_1}\cdots p_{\lambda_k}\};$$

$$\lambda = (\lambda_1,\ldots,\lambda_k) \in Par$$

are each additive bases for Λ.

See Stanley (2001) for a proof.

1.1.1 Plethysm

Definition 1.5. *Let $f \in \Lambda$ be the sum of monomials $\sum_{i\geq 0} x^{\alpha_i}$. The plethysm $g[f]$ is defined as*

$$g[f] = g(x^{\alpha_1}, x^{\alpha_2}, \ldots).$$

Although this appears to depend on the order that the monomials of f are summed, the operation is in fact well defined because g is symmetric, hence any reordering of the terms in f yield the same result. The plethysm $g[f]$ is sometimes written as $f \circ g$, because in certain contexts the operation really is composition. We will not use that notation. In general, the plethystic expression $g[f]$ is only defined when the number of monomials in f equals the number of variables in g.

Example 1.1. *Consider the power symmetric function p_k and the arbitrary symmetric function f from definition* 1.5. *Then*

$$f[p_k] = f(x_1^k, x_2^k, \ldots) = \sum_{i\geq 0} x^{\alpha_i k} = p_k[f].$$

It is clear that

$$(af + bg)[h] = af[h] + bg[h] \text{ and}$$
$$(fg)[h] = f[h] \cdot g[h],$$

so with example 1.1 we can define the plethysm for any functions by using the power sum symmetric basis. In particular, if $g = \sum_\lambda c_\lambda p_\lambda$ where the c_λ are scalars, then

$$g[f] = \sum_\lambda c_\lambda p_\lambda[f] = \sum_\lambda c_\lambda \prod_{i=1}^{\ell(\lambda)} f(x_1^{\lambda_1}, x_2^{\lambda_2}, \ldots).$$

1.2 The Zeta Function of a Curve

To study the numbers N_s of points on a curve C over the finite field F_{q^s}, we consider the generating function $\sum_{s\geq 1} N_s u^s$. As with the case of symmetric functions, we will deal with these as formal power series.

Definition 1.6. *The zeta function of a curve C is given by the series*

$$Z_C(u) = \exp\left(\sum_{s=1}^{\infty} \frac{N_s u^s}{s}\right),$$

where we are using the identity $\exp(u) = \sum_{s\geq 0} u^s/s!$.

Although the zeta function essentially encodes the same information as $\sum_{s\geq 1} N_s u^s$, it turns out that the zeta function is more convenient to work with.

Example 1.2. *Consider the circle at infinity in the finite projective plane, i.e. $z = 0$. By definition, this is the set of points $(x, y, 0) \in \mathbb{P}^2(F_{q^s})$, and the number of such* *points equals the number of points in* $\mathbb{P}^1(F_{q^s})$*. Therefore* $N_s = q^s + 1$*, so*

$$\begin{aligned}\sum_{s=1}^{\infty} \frac{N_s u^s}{s} &= \sum_{s=1}^{\infty} \frac{(q^s+1)u^s}{s} \\ &= \left(\sum_{s=1}^{\infty} \frac{u^s}{s}\right) + \left(\sum_{s=1}^{\infty} \frac{q^s u^s}{s}\right) \\ &= -\ln(1-u) - \ln(1-qu) \\ &= -\ln((1-u)(1-qu)).\end{aligned}$$

The third line follows from the identity $\sum_{s\geq 1} w^s/s = -\ln(1-w)$*. Hence*

$$Z_z(u) = \frac{1}{(1-u)(1-qu)}.$$

A key feature of this function is that it is rational with integer coefficients. This leads us to an important theorem regarding the enumeration of points on elliptic curves.

Theorem 1.1. (*Weil*) *Let* $f(x,y,z) \in F_{q^s}[x,y,z]$ *be a nonzero, nonsingular homogeneous polynomial. Then*

$$Z_f(u) = \frac{P(u)}{(1-u)(1-qu)}$$

where $P(u)$ *is a polynomial with integer coefficients, with degree equaling twice the genus of the curve, and* $P(0) = 1$*.*

Recall that a polynomial is nonsingular if the curve it defines has a unique tangent line at every point, and also that the genus of a curve is defined as $g = \frac{1}{2}(d-1)(d-2)$.

Corollary. *If E is an elliptic curve, then*

$$Z_E(u) = \frac{1-(\alpha_1+\alpha_2)u+\alpha_1\alpha_2 u^2}{(1-u)(1-qu)}.$$

Chapter 2

Enumerating Points on Elliptic Curves

A motivating result for our forthcoming investigation is that, for an algebraic curve of genus g, the number of points over the finite fields $F_q, F_{q^2}, \ldots, F_{q^g}$ is sufficient data to determine the number of points over any higher field extension. This leads one to question how exactly the points over these higher field extensions relate to those over the first g. In the remaining discussion we will focus on the case $g = 1$.

2.1 Preliminary Results

In the background section we have already begun to touch upon the enumeration of points on algebraic curves. Combining definition 1.6 with the corollary of theorem 1.1, it is seen by equating coefficients that $N_k = 1+q^k-\alpha_1^k-\alpha_2^k$. Or, in plethystic notation, $N_k = p_k[1+q-\alpha_1-\alpha_2]$. Since the case $k = 1$ yields the relation $\alpha_1 + \alpha_2 = 1 + q - N_1$, it follows that q and N_1 fully determine all N_k.

Theorem 2.1 (Garsia).

$$N_k = \sum_{i=1}^{k} (-1)^{i-1} P_{i,k}(q) N_1^i$$

where the $P_{i,k}$ are polynomials with positive integer coefficients.

The $P_{i,k}$ in fact relate directly to wheel graphs and their spanning trees. In particular, the quantity $1 + q^k - N_k$ can be shown to satisfy the same recurrence relation as a generalization of the Lucas numbers. A bijection is then established between the generalized Lucas numbers and the spanning trees of a wheel graph. See Musiker (2007) for details.

Other aspects of the zeta function yield combinatorial identities as well. For instance, using the symmetric function identity

$$\exp\left(\sum_{k\geq 1}\frac{p_k u^k}{k}\right)=\frac{1}{\sum_{k\geq 0}(-1)^k e_k u^k}$$

and the fact that $N_k = p_k[1+q-\alpha_1-\alpha_2]$, we can write the zeta function as

$$Z_E(u)=\frac{1}{\sum_{k\geq 0}(-1)^k E_k u^k}$$

where $E_k = e_k[1+q-\alpha_1-\alpha_2]$. It turns out that the E_k can be obtained by evaluating a bivariate polynomial generalization of the Fibonacci numbers at the point $(q,-N_1)$. So like the N_k, the E_k also have a natural formula in terms of q and N_1. A proof of this is also given in Musiker (2007). Lastly, consider the symmetric function identity

$$\exp\left(\sum_{k\geq 1}\frac{p_k u^k}{k}\right)=\sum_{k\geq 0}h_k u^k.$$

Following the above reasoning, the zeta function has yet another form

$$Z_E(u)=\sum_{k\geq 0}H_k u^k$$

where $H_k = h_k[1+q-\alpha_1-\alpha_2]$.

2.2 (q,t)-Wheel Graphs

As mentioned above, the equation in Theorem 2.1 leads to a connection with wheel graphs. We define the (q,t)-wheel graph on $k+1$ vertices by the following construction. Begin with the cycle graph on k vertices, with edges directed counter-clockwise. Then include an additional central vertex, which is attached by t bidirectional spokes to each rim vertex. Lastly, attach q clockwise edges between each pair of adjacent rim vertices. This construction will be denoted by $W_k(q,t)$. See Fig. 2.1 for an example.

With this construction, Theorem 2.1 may be restated very cleanly.

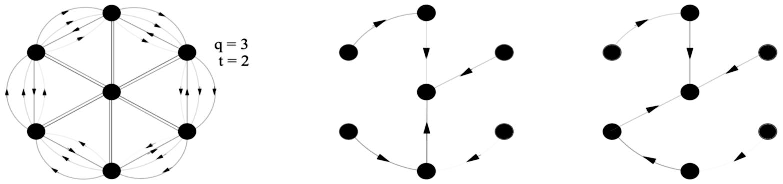

Figure 2.1 The (q,t)-wheel graph $W_6(3,2)$ and two directed spanning trees with central roots.

Theorem 2.2. *Let $\mathcal{W}_k(q,t)$ denote the number of directed spanning trees of $W_k(q,t)$ with all edges directed towards the central vertex. Then*

$$N_k = -\mathcal{W}_k(q,-N_1).$$

The expression $-\mathcal{W}_k(q,-N_1)$ does not admit the same enumerative interpretation as given above, because it would refer to a graph containing negative numbers of edges. This result is in similar spirit to a theorem due to R.P. Stanley, which gives a combinatorial interpretation to the evaluation of a graph's chromatic polynomial on negative integers. In particular, $|\chi(-1)|$ equals the number of acyclic orientations of the graph. See Stanley (1972) for details.

In light of the generating function identities obtained in section 2.1, Theorem 2.2 suggests an analogous investigation of the generating function

$$W_{q,t}(u) = \exp\left(\sum_{k=1}^{\infty} \frac{\mathcal{W}_k(q,t)u^k}{u}\right).$$

Using Theorem 2.2 and the corollary of Theorem 1.1,

$$\begin{aligned} W_{q,N_1}(u) &= \frac{1}{\exp\left(\sum_{k=1}^{\infty} \frac{N_k|_{N_1\to -N_1} u^k}{u}\right)} \\ &= \frac{(1-u)(1-qu)}{1-(1+q+N_1)u+qu^2} \end{aligned}$$

where in the second step N_k is to be viewed as a function of N_1. Factoring the denominator as $1-(1+q+N_1)u+qu^2 = (1-\beta_1 u)(1-\beta_2 u)$, we can expand the generating function as a product of two geometric series. Matching coefficients then yields

$$\mathcal{W}_k(q,N_1) = (-1)^k + (-q)^k + \beta_1^k + \beta_2^k = p_k[-1-q+\beta_1+\beta_2];$$

note the similarity compared to $N_k = p_k[1+q-\alpha_1-\alpha_2]$. The same generating function identities used in section 2.1 can also be applied to express E_k and H_k in terms of this "alphabet" $-1-q+\beta_1+\beta_2$. The results are compiled in the following table.

	Elliptic Curves	(q,t)-Wheel Graphs
Exponential generating function	$\frac{1-(1+q-N_1)u+qu^2}{(1-u)(1-qu)}$	$\frac{(1-u)(1-qu)}{1-(1+q+N_1)u+qu^2}$
Alphabet	$1+q-\alpha_1-\alpha_2$	$-1-q+\beta_1+\beta_2$
N_k ($\mathcal{W}_k$ for wheel graphs)	$p_k[1+q-\alpha_1-\alpha_2]$	$p_k[1+q-\alpha_1-\alpha_2]$
H_k	$h_k[1+q-\alpha_1-\alpha_2]$	$(-1)^{k-1}e_k[1+q-\alpha_1-\alpha_2]$
E_k	$e_k[1+q-\alpha_1-\alpha_2]$	$(-1)^k h_k[1+q-\alpha_1-\alpha_2]$

Chapter 3

Elliptic Curves and Critical Groups of Wheel Graphs

The previous chapter connected elliptic curves to wheel graphs by equating their numbers of points and spanning trees, respectively. Recall, however, that to establish this equivalence we had to construct "graphs" with negative numbers of edges. Thus the most basic description using a vertex set and edge set does not apply, but matrix representations are perfectly admissible. This chapter is largely devoted to the relation between these matrix representations and elliptic curves.

3.1 Elliptic Curve Hierarchy

Several key properties of elliptic curves have analogous statements concerning critical groups (as yet undefined) of wheel graphs. These properties of elliptic curves are now briefly described.

Let E be an elliptic curve (over an unspecified field) and $q = p^k$ for some prime p and positive integer k. Recall that there is an inclusion of fields

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

whenever the divisibilities $k_i | k_{i+1}$ hold, and where $\overline{\mathbb{F}_p}$ is the algebraic closure of $\mathbb{F}_q$. This implies a subgroup series

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

with the same divisibility constraints $k_i | k_{i+1}$. One more important feature is the Frobenius endomorphism $\phi : x \mapsto x^q$, which is an element of (and in fact generates) the Galois group $\mathrm{Gal}(\mathbb{F}_{q^\ell}/\mathbb{F}_q)$. Since ϕ must fix the ground field, extending this map to act on points by $\phi : P = (x, y) \mapsto (x^q, y^q)$ has the property that

$$\phi^k(P) = P \text{ if and only if } P \in E(\mathbb{F}_{q^k}).$$

In other words, each group $E(\mathbb{F}_{q^k})$ can be defined by $\ker(1 - \phi^k)$. See Silverman (2009) for a more detailed discussion.

3.2 Critical Groups

Let $G = (V, E)$ be a (possibly) directed graph, $A(G)$ be the usual adjacency matrix of G, and $\Delta(G)$ be the diagonal matrix such that $\Delta(G)_{vv}$ is the out-degree of vertex v. ($\Delta(G)$ is usually referred to as the degree matrix of G.) The Laplacian is defined as $Q(G) = \Delta(G) - A(G)$.

Definition 3.1. *The critical group $\mathcal{K}(G)$ of a graph G is the cokernel of the transpose of the Laplacian $Q(G)$ acting on $\mathbb{Z}^{|V|}$:*

$$\mathcal{K}(G) := \operatorname{coker} Q(G)^T = \mathbb{Z}^{|V|}/Q(G)^T\mathbb{Z}^{|V|}.$$

The dual critical group of G is similarly defined to be $\mathcal{K}^*(G) := \operatorname{coker} Q(G)$.

Definition 3.2. *The reduced critical group $K(G)$ of G is the torsion subgroup of $\mathcal{K}(G)$. Similarly, the reduced dual critical group $K^*(G)$ is the torsion subgroup of $\mathcal{K}^*(G)$.*

The relationship between a graph and the structure of its critical group is, in general, not well understood. There exist, however, well-behaved examples. See Biggs (1999) for a complete classification in the case of simple wheel graphs.

Definition 3.3. *Let $G = (V, E)$ be a digraph and $\pi = (\pi_1, \dots, \pi_p)$ be an ordered partition of V. The partition π is said to be* equitable *for G if there exist nonnegative integers F_{ij} and R_{ij} for all $1 \le i, j \le p$ such that every vertex in π_i is the initial vertex of exactly F_{ij} edges having terminal vertices in π_j, and every vertex in π_j is the terminal vertex of exactly R_{ij} edges with initial vertex in π_i.*

Definition 3.4. *Let G be a digraph and π be an equitable partition of G. The quotient of G by π, denoted G/π, is the graph whose adjacency matrix is given by F_{ij}.*

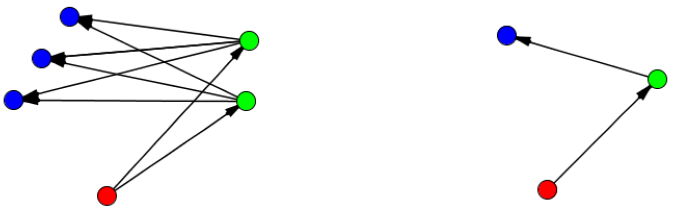

Figure 3.1 A digraph (left) and its quotient (right) by an equitable partition marked by vertex color.

Figure 3.1 illustrates an example of a directed graph and its quotient by an equitable partition. Not surprisingly, the critical groups of a graph and one of its quotients are related. The following theorem makes this precise.

Theorem 3.1 (Wagner)**.** *Let $G = (V, E)$ be a strongly connected graph and $\pi = \{\pi_1, \dots, \pi_p\}$ be an equitable partition of G. Then there exists a natural injective homomorphism $\psi : \mathcal{K}(G/\pi) \to \mathcal{K}(G)$ given by $\psi(x) = Px$, where P is the $V \times \{1, \dots, p\}$ matrix with entries*

$$P_{vi} = \begin{cases} 1 & \textit{if } v \in \pi_i, \\ 0 & \textit{if } v \notin \pi_i. \end{cases}$$

The restriction of ψ to the torsion subgroup $\psi|_{tor} : K(G/\pi) \to K(G)$ is also injective.

Under the hypotheses of Theorem 3.1, $\mathcal{K}(G/\pi)$ may be regarded as a subgroup of $\mathcal{K}(G)$ with the inclusion ψ.

3.3 Critical Groups of (q, t)-Wheel Graphs

Throughout this section, we will denote $K(W_k(q, t))$ by $K(k, q, t)$. Our general aim is to map properties of the sequence $\{K(k, q, t)\}_{k\geq 1}$ onto those of elliptic curves given above.

In Musiker (2009), Musiker defines the critical group of a wheel graph using not the Laplacian Q, but the reduced Laplacian Q_0 obtained by deleting the row and column corresponding to the central vertex. This structure is manifestly not the critical group of any graph, but is in fact isomorphic to the reduced critical group.

Proposition 3.1. *The "critical group" defined using the reduced Laplacian Q_0 of a wheel graph $W_k(q,t)$ is isomorphic to the reduced critical group $K(k,q,t)$.*

$$\operatorname{coker}(Q_0^T(W_k(q,t))) \cong K(k,q,t).$$

Proof. For a wheel graph $W_k(q,t)$, the Laplacian is given by the $(k+1)\times(k+1)$ matrix

$$Q = \begin{bmatrix} 1+q+t & -q & 0 & \cdots & 0 & -1 & -t \\ -1 & 1+q+t & -q & 0 & \cdots & 0 & -t \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & -t \\ 0 & \cdots & -1 & 1+q+t & -q & 0 & -t \\ 0 & \cdots & 0 & -1 & 1+q+t & -q & -t \\ -q & 0 & \cdots & 0 & -1 & 1+q+t & -t \\ -t & -t & -t & \cdots & -t & -t & kt \end{bmatrix},$$

where the last row and column correspond to the central vertex. By adding the first k rows to the last row, and then the first k columns to the last column, we obtain the matrix

$$Q' = \begin{bmatrix} 1+q+t & -q & 0 & \cdots & 0 & -1 & 0 \\ -1 & 1+q+t & -q & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & -1 & 1+q+t & -q & 0 & 0 \\ 0 & \cdots & 0 & -1 & 1+q+t & -q & 0 \\ -q & 0 & \cdots & 0 & -1 & 1+q+t & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}.$$

Since Q and Q' are related by invertible matrices, $\operatorname{coker}(Q^T) \cong \operatorname{coker}(Q'^T)$. Note also that the image of Q'^T is isomorphic to the image of Q_0^T, the only formal difference being the presence of a zero in the last entry of every element in Im Q'^T. It follows that $\operatorname{coker}(Q'^T) \cong \operatorname{coker}(Q_0^T) \oplus \mathbb{Z}$, thus

$$\mathcal{K}(W_k(q,t)) \cong \operatorname{coker}(Q_0^T) \oplus \mathbb{Z}.$$

In Musiker (2009) it is shown that $\operatorname{coker}(Q_0^T)$ has finite order, and therefore must be isomorphic to the reduced critical group. □

Proposition 3.2. *Let E be an elliptic curve and N_k be the number of points of E over the finite field $\mathbb{F}_{q^k}$. Then Theorem 2.2 is equivalent to $N_k = |K(k,q,-N_1)|$.*

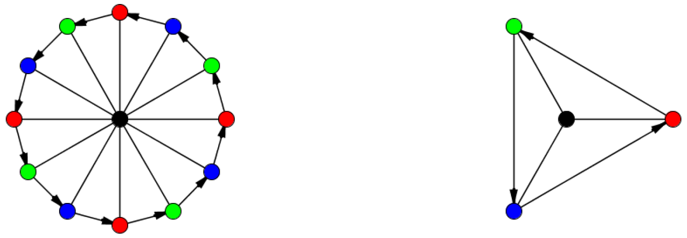

Figure 3.2 A wheel graph $K(12, 0, 1)$ (left) and its quotient $K(3, 0, 1)$ (right) by a partition using $l = 3$ parts marked by color.

Proof. The Matrix-Tree theorem tells us that for a connected, undirected graph G, the order of $K(G)$ equals the number of spanning trees of G. A slight extension of this theorem shows that for a digraph G and reduced Laplacian $Q_v(G)$ obtained by deleting the row and column associated with vertex v, the order of $\operatorname{coker}(Q_v^T)$ is equal to the number of directed spanning trees of G with sink v.

From Prop. 3.1 it follows that $|\operatorname{coker}(Q_0^T)| = |K(k, q, t)|$, and then substituting $t \to -N_1$ yields the desired result. □

We now turn our attention to the structure of $\{K(k, q, t)\}_{k \geq 1}$ itself. Recall Theorem 3.1, which provides an injective homomorphism between critical groups whenever one of their associated graphs is a quotient of the other. There are in fact very natural equitable partitions on wheel graphs; in particular, if l divides the number of rim vertices k, then we can form parts by walking around the rim and repeatedly counting off to l so that each part contains k/l vertices. The hub vertex comprises its own part. Taking the quotient by this partition yields another wheel graph with l rim vertices. See Figure 3.2 for an example.

This implies the existence of an injective homomorphism

$$\psi_{k_2,k_1} : K(k_1, q, t) \to K(k_2, q, t)$$

whenever k_1 divides k_2. As mentioned above, we may thus view $K(k_1, q, t)$ as a subgroup of $K(k_2, q, t)$ when $k_1 \mid k_2$. This is the exact partial ordering as given for elliptic curves, where $E(\mathbb{F}_{q_1^k}) \leq E(\mathbb{F}_{q_2^k})$ precisely when $k_1 \mid k_2$.

By definition of the map ψ given in Theorem 3.1, we have $\psi_{k_3,k_2} \circ \psi_{k_2,k_1} = \psi_{k_3,k_1}$. Therefore we can form the direct limit

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

so that every critical group $K(k,q,t)$ may be naturally identified with a subgroup of $\overline{K}(q,t)$. This direct limit is analogous to the field $\overline{\mathbb{F}_p}$. Closer examination of the maps ψ_{k_2,k_1} reveals that they simply repeat the input vector k_2/k_1 times. One is then lead to view $\overline{K}(q,t)$ as the set of all periodic vectors $w = (\ldots, w_{-1}, w_0, w_1, \ldots)$, so that the subgroup of $\overline{K}(q,t)$ isomorphic to $K(k,q,t)$ is all the vectors of period k.

Define the shift map $\rho : \overline{K}(q,t) \to \overline{K}(q,t)$ by

$$\rho(\ldots, w_{i-1}, w_i, w_{i+1}, \ldots) = (\ldots, w_{i-2}, w_{i-1}, w_i, \ldots).$$

Then a theorem due to Musiker states that for all $k \geq 1$, $q \geq 0$, and $t \geq 1$,

$$K(k,q,t) \cong \text{Ker}(1 - \rho^k).$$

The results of this chapter are summarized by the following correspondences:

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

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

The reader may be left wondering what can be said regarding the internal structure of $K(k,q,t)$ as compared to that of $E(\mathbb{F}_{q^k})$. We end the chapter with a theorem addressing a only special case of this question, albeit in a very satisfying way.

Theorem 3.2. *Let E be an elliptic curve with endomorphism ring $End(E) \cong \mathbb{Z}[\pi]$, where π is the Frobenius map. As before, $N_1 = |E(\mathbb{F}_q)|$. Then*

$$E(\mathbb{F}_{q^k}) \cong K(k,q,-N_1).$$

For a proof of this, see Musiker (2009).

Bibliography

Biggs, N.L. 1999. Chip-firing and the critical group of a graph. *Journal of Algebraic Combinatorics* 9.

Ireland, Kenneth, and Michael I. Rosen. 1972. *Elements of Number Theory: Including an Introduction to Equations over Finite Fields*. New York: Bogden and Quigley, Inc.

Musiker, Gregg. 2007. Combinatorial aspects of elliptic curves. *Seminaire Lotharingien de Combinatoire* 56.

———. 2009. The critical groups of a family of graphs and elliptic curves over finite fields. *Journal of Algebraic Combinatorics* 30.

Silverman, Joseph H. 2009. *The Arithmetic of Elliptic Curves*. New York: Springer.

Silverman, Joseph H., and John Tate. 2010. *Rational Points on Elliptic Curves*. New York: Springer.

Stanley, R. P. 1972. Acyclic orientations of graphs. *Discrete Mathematics* 5.

Stanley, Richard P. 2001. *Enumerative Combinatorics*, vol. 2. Cambridge: Cambridge University Press.

Wagner, David G. 2000. The critical group of a directed graph. *ArXiv Mathematics e-prints* math/0010241.