Formal Power Series and Algebraic Combinatorics
Séries Formelles et Combinatoire Algébrique
Tianjin, China 2007

Elliptic Curve Groups and Chip-Firing Games

Gregg Musiker

Abstract. The author illustrates several results from the theory of elliptic curves, as well as the theory of chip-firing games on graphs. More specifically, in both of these cases, we obtain analogues of cyclotomic polynomials with several combinatorial and number theoretic properties. We also provide an analysis of zeta functions which highlights the connections between these two disparate fields.

Résumé. L'auteur illustre plusieurs résultats de la théorie de courbes elliptiques, aussi bien que la théorie de jeux de *chip-firing* sur des graphiques. Plus spécifiquement, en tous les deux cas, nous obtenons des analogues des polynômes cyclotomiques avec plusieurs propriétés théorétiques combinatoires et de nombre. Nous fournissons également une analyse des fonctions de zéta qui accentue les raccordements entre ces deux champs disparates.

1. Introduction

The theory of elliptic curves is quite rich, arising in both complex analysis and number theory. In particular, they can be given a group structure using the tangent-chord method or the divisor class group of algebraic geometry [**11**]. This property makes them not only geometric but also algebraic objects and allows them to be used for cryptographic purposes [**15**].

In [**8**], the author started an exploration of elliptic curves from a combinatorial viewpoint. For a given elliptic curve E defined over a finite field $\mathbb{F}_q$, we let $N_k = \#E(\mathbb{F}_{q^k})$ where $\mathbb{F}_{q^k}$ is a kth degree extension of the finite field $\mathbb{F}_q$. Because the zeta function for E, i.e.

$$\exp\left(\sum_{k\geq 1}\frac{N_k}{k}t^k\right) = \frac{1-(1+q-N_1)t+qt^2}{(1-t)(1-qt)},$$

only depends on q and N_1, the sequence $\{N_k\}$ only depends on those numbers as well. More specifically, we observe that these bivariate expressions for N_k are in fact polynomials with integer coefficients, which alternate in sign with respect to the power of N_1 [**2**].

This motivated the main topic of [**8**], which was the search for a combinatorial interpretation of these coefficients. One such interpretation involved spanning trees of a certain family of graphs, and to better describe these, we introduce some graph theory terminology. The wheel graph W_k is defined to be the cycle graph on k vertices with the addition of one extra vertex which is adjacent to all other vertices. A spanning tree of such a graph is a connected subgraph which includes all $k+1$ of the vertices but does not contain any cycles. In particular, such a tree consists of a sequence of disconnected arcs along the rim, in addition to a series of spokes emanating out from the central vertex. Furthermore, we define the (q,t)-wheel graph as a directed multi-graph version of the wheel graph. Each spoke is replaced with $2t$ directed edges, with half going towards the hub, and half going away from it. Also, each edge between two adjacent rim vertices is replaced with $q+1$ directed edges. Out of these edges, q of them are oriented clockwise, and the last one goes counter-clockwise.

2000 *Mathematics Subject Classification.* Primary 68R15; Secondary 11G07.

Key words and phrases. chip-firing games, cyclic languages, elliptic curves, finite fields, spanning trees, zeta functions.

This work was supported by the NSF, grant DMS-0500557. The author would like to thank Adriano Garsia for his guidance and Christophe Reutenauer for many useful conversations.

Let $\mathcal{W}_k(q,t)$ denote the number of rooted directed spanning trees of (q,t)-wheel graph on $k+1$ vertices, which are rooted at the central hub. We get the following equality, which relates $\mathcal{W}_k(q,t)$ to the N_k's, thus giving a combinatorial description of the coefficients.

THEOREM 1.

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

for all $k \geq 1$.

PROOF. See [**8**] for three different proofs of this result. We will summarize the third such proof in Section 2.3. □

This motivates a closer examination of the relationship between points on an elliptic curve E over $\mathbb{F}_{q^k}$ and spanning trees on the wheel graph W_k.

In this write-up we continue this journey. An elliptic curve E has an abelian group structure, and indeed the set of spanning trees of a graph also has a natural abelian group structure. Here we study one isomorphic to the critical group of the graph, which has ties to the theory of chip-firing games and abelian sandpile models of dynamical systems. While in [**8**], we focused on the relationship between the integer sequences $\{N_k\}$ and $\{\mathcal{W}_k(q,N_1)\}$, here we compare these two group structures, illustrating that the connections between elliptic curves and spanning trees run even deeper than earlier observed. Numerous theorems which are true for elliptic curve groups have analogues in terms of critical groups of the (q,t)-wheel graph.

Additionally the theory of critical groups will also allow us to re-interpret the group elements as the set of admissible words for a primitive circuit in a specific non-deterministic finite automaton. As an application, we will then compare the zeta function of an elliptic curve and the zeta function of the corresponding cyclic language.

2. Determinantal formula for N_k

We will shortly describe more fully the relationship between the group structure of elliptic curves and critical groups, but first illustrate a couple applications of Theorem 1. These results will be useful later on when comparing the groups, and additionally are interesting for their own sake. Our first application is a determinantal formula for N_k by utilizing the Matrix-Tree theorem [**13**].

THEOREM 2. *Let* $M_1 = [-N_1]$, $M_2 = \begin{bmatrix} 1+q-N_1 & -1-q \\ -1-q & 1+q-N_1 \end{bmatrix}$, *and for* $k \geq 3$, *let* M_k *be the* k*-by-*k *"three-line" circulant matrix*

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

Then the sequence of integers $N_k = \#E(\mathbb{F}_{q^k})$ *satisfies the relation*

$$N_k = -\det M_k$$

for all $k \geq 1$. *We obtain an analogous determinantal formula for* $\mathcal{W}_k(q,t)$, *in fact* $\mathcal{W}_k(q,t) = \det M_k|_{N_1=-t}$.

We provide two proofs of this theorem, one which relies on graph theory, and one which introduces a new sequence of polynomials which have intriguing number theoretic and combinatorial properties.

2.1. First proof of Theorem 2: Via graph theory. We appeal to the directed multi-graph version of the Matrix-Tree Theorem to count the number of spanning trees of (q,t)-W_k with root given as the hub.

We obtain Laplacian matrix

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

where the last row and column correspond to the hub vertex, which happens to be the root. By the Matrix-Tree theorem, the number of directed rooted spanning trees is $\det L_0$ where L_0 is matrix L with the last row and last column deleted. We have the identities

$$\begin{aligned} N_k &= -\mathcal{W}_k(q, -N_1) \\ M_k &= L_0\Big|_{t=-N_1} \quad \text{and thus} \\ \mathcal{W}_k(q,t) &= \det L_0 \quad \text{implies} \\ -\mathcal{W}_k(q,-N_1) &= -\det L_0\Big|_{t=-N_1} \quad \text{so we get} \\ N_k &= -\det M_k. \end{aligned}$$

Thus we have proven Theorem 2.

2.2. Combinatorial aspects of matrix M_k. The matrices M_k each have an especially elegant Smith normal form. Recall that such a form is unchanged by

(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.

PROPOSITION 1. *For any specific choice of integers q and N_1, the Smith normal form of M_k is an integral diagonal matrix with $(k-2)$ or $(k-1)$ ones on the diagonal. More generally, if we preserve q and N_1 as variables, then the Smith normal form of M_k is* equivalent *to a matrix with $(k-2)$ ones on the diagonal, followed by a 2-by-2 block whose entries consist of integral polynomials in q and N_1. All other entries are zero.*

PROOF. To begin, we note after permuting rows cyclically and multiplying through all rows by (-1) that we get

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

Since this matrix is lower-triangular with ones on the diagonal, besides the upper-right corner of three, we can add a multiple of the first row to the second and third rows, respectively, and obtain a new matrix with vector

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

as the first column. Since we can add multiples of columns to one another as well, we also obtain a matrix with vector V^T 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 the 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 down one row. 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 which will be more complicated. □

One can go further than Proposition 1 and explicitly construct the entries in the last two rows and columns. For this analysis, we use a slight variant of the bivariate Fibonacci polynomials as defined in [**8**].

DEFINITION 1. *The* $(2k+1)st$ **Fibonacci polynomial** *is*

$$E_k(q,N_1) = (-1)^k \sum_{S\subseteq\{1,2,\ldots,2k-2\} \ : \ S\cap(S_1^{\{2k-1\}}-\{1\})=\phi} q^{\#\text{ even elements in } S}\ (-N_1)^{k-\#S}.$$

This sum is over sets S *with no (linearly) consecutive elements.*

With these bivariate Fibonacci polynomials E_k in mind, we can identity the polynomials occurring in the 2-by-2 block.

THEOREM 3. *The Smith normal form of* M_k *is equivalent to*

$$\begin{bmatrix} 1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 & 0 \\ 0 & 0 & \ldots & 0 & qE_{k-1}/N_1 - 1 & -qE_k/N_1 \\ 0 & 0 & \ldots & 0 & E_k/N_1 & -E_{k+1}/N_1 - 1 \end{bmatrix}.$$

Note that this 2*-by-*2 *block will reduce to* $\begin{bmatrix} m_1 & 0 \\ 0 & m_2 \end{bmatrix}$ *such that* $m_1|m_2$ *as integers once* q *and* N_1 *are evaluated as specific numbers.*

PROOF. We consider a recursive argument by comparing the Fibonacci recurrence with identities arising from reduction to Smith normal form. Details given in [**8**]. □

2.3. Second proof of Theorem 2 and introduction to Elliptic Cyclotomic polynomials. Alternatively, we note that we can factor

$$N_k = 1 + q^k - \alpha_1^k - \alpha_2^k$$

using the fact that $q = \alpha_1\alpha_2$. Consequently,

$$N_k = (1-\alpha_1^k)(1-\alpha_2^k)$$

and we can factor each of these two terms using cyclotomic polynomials. We recall that $(1-x^k)$ factors as

$$1 - x^k = \prod_{d|k} Cyc_d(x)$$

where $Cyc_d(x)$ is a monic irreducible polynomial with integer coefficients. We can similarly factor N_k as

$$N_k = \prod_{d|k} Cyc_d(\alpha_1)Cyc_d(\alpha_2).$$

These factors are therefore bivariate analogues of the cyclotomic polynomials, and we will refer to them henceforth as **elliptic cyclotomic polynomials**, denoted as $ECyc_d$. More specifically

DEFINITION 2. *We define the elliptic cyclotomic polynomials to be the sequence of polynomials in variables* q *and* N_1 *such that for* $d \geq 1$*,*

$$ECyc_d = Cyc_d(\alpha_1)Cyc_d(\alpha_2),$$

where α_1 *and* α_2 *are the two roots of*

$$T^2 - (1 + q - N_1)T + q.$$

We verify that they can be expressed in terms of q *and* N_1 *by the following proposition.*

PROPOSITION 2. *Writing down* $ECyc_d$ *in terms of* q *and* N_1 *yields irreducible bivariate polynomials with integer coefficients.*

PROOF. Integrality follows from the Fundamental Theorem of Symmetric Functions that states that a symmetric polynomial with integer coefficients can be rewritten as an integral polynomial in $e_1, e_2, \ldots$. In this case, $Cyc_d(\alpha_1)Cyc_d(\alpha_2)$ is a symmetric polynomial in two variables so $e_1 = \alpha_1 + \alpha_2 = 1 + q - N_1$, $e_2 = \alpha_1\alpha_2 = q$, and $e_k = 0$ for all $k \geq 3$. Thus we obtain an expression for $ECyc_d$ as a polynomial in q and N_1 with integer coefficients. For the proof of why these are irreducible, see [**8**]. □

We can factor N_k, i.e. the $ECyc_d$'s even further, if we no longer require our expressions to be integral.

$$N_k = \prod_{j=1}^{k}(1 - \alpha_1\omega_k^j)(1 - \alpha_2\omega_k^j) \tag{1}$$

$$= \prod_{j=1}^{k}(1 - (\alpha_1 + \alpha_2)\omega_k^j + (\alpha_1\alpha_2)\omega_k^{2j}) \tag{2}$$

$$= (-1)\prod_{j=1}^{k}(-\omega_k^{k-j})(1 - (1 + q - N_1)\omega_k^j + (q)\omega_k^{2j}) \tag{3}$$

$$= -\prod_{j=1}^{k}\left((1 + q - N_1) - q\omega_k^j - \omega_k^{k-j}\right). \tag{4}$$

Furthermore, the eigenvalues of a circulant matrix are well-known, and involve roots of unity analogous to the expression precisely given by (2). (For example Loehr, Warrington, and Wilf [**6**] provide an analysis of a more general family of three-line-circulant matrices from a combinatorial perspective. Using their notation, our result can be stated as

$$N_k = \Phi_{k,2}(1 + q - N_1, -q)$$

where $\Phi_{p,q}(x, y) = \prod_{j=1}^{p}(1 - x\omega^j - y\omega^{qj})$ and ω is a primitive pth root of unity. It is unclear how our combinatorial interpretation of N_k, in terms of spanning trees, relates to theirs, which involves permutation enumeration.) In particular, we prove Theorem 2 since $\det M_k$ equals the product of M_k's eigenvalues, which are precisely given as the k factors of $-N_k$ in equation (2). This argument gives us a proof of Theorem 1 as well.

The sequence of elliptic cyclotomic polynomials motivates several avenues for further exploration. For example, the author has been able to show that they have degrees in q and in N_1 equal to the degrees of the ordinary cyclotomic polynomials (for $k \geq 2$), and has investigated their values at formal evaluations of N_1 such as $N_1 = 0$ or $2q + 2$ [**8**]. Another tie to ordinary cyclotomic polynomials is demonstrated by the following remarkable geometric interpretation of the elliptic cyclotomic polynomials.

THEOREM 4.

$$ECyc_d = \left| Ker\left(Cyc_d(\pi)\right) : \ E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})\right|$$

where π denotes the Frobenius map, and $Cyc_d(\pi)$ is an element of $End(E) = End(E(\overline{\mathbb{F}_q}))$.

PROOF. See [**8**] □

3. Introduction to chip-firing games

We now switch topics and discuss some fundamental results from the theory of chip-firing games on graphs. The main source for these details is [**1**], though there is an extensive literature on the subject. At first glance, this topic might appear totally unrelated to elliptic curves, but we will shortly flesh out the connection. Given a directed (loop-less) graph G, we define a configuration C to be a vector of nonnegative integers, with a coordinate for each vertex of the graph. Thus we let C_i denote the integer corresponding to vertex v_i. One can think of this assignment as a collection of chips placed on each of the vertices. We say that a given vertex v_i can *fire* if the number of chips it holds, C_i, is greater than or equal to its out-degree. If so, firing leads to a new configuration where a chip travels along each outgoing edge incident to v_i. Thus we obtain a configuration C' where $C'_j = C_j + d(v_i, v_j)$ and $C'_i = C_i - d(v_i)$. Here $d(v_i, v_j)$ equals the number of directed edges from v_i to v_j, and $d(v_i)$ is the out-degree of v_i, which of course equals $\sum_{j \neq i} d(v_i, v_j)$.

Many interesting problems arise from this definition. For example, it can be shown [**4**] that the set of configurations reachable from an initial choice of a vector forms a distributive lattice. For the purposes of

relating this topic to an elliptic curve, we will consider a variant of the standard chip-firing game, known as the **dollar game**. In the dollar game, we have the same set-up as before with three changes.

(1) We designate one vertex v_0 to be the bank, and allow C_0 to be negative. All the other C_i's still must be nonnegative.
(2) To limit extraneous configurations, we presume that the sum $\sum_{i=0}^{\#V-1} C_i = 0$. (Thus in particular, C_0 will be non-positive.)
(3) The bank, i.e. vertex v_0, is only allowed to fire if no other vertex can fire. Note that since we now allow C_0 to be negative, v_0 is allowed to fire even when it is smaller than its outdegree, and thus this rule completely determines when v_0 can fire.

With this set-up in mind, we define a configuration to be **stable** if v_0 is the only vertex that can fire. We define a configuration C to be **recurrent** if there is firing sequence which will lead back to C. Note that this will necessarily require the use of v_0 firing. We call a configuration **critical** if it is both stable and recurrent.

THEOREM 5. [**1**] *For any initial configuration satisfying rules (1) and (2) above,there exists a* unique *critical configuration that can be reached by a firing sequence, subject to rule (3).*

We define the **critical group of graph** G, with respect to vertex v_0 to be the set of critical configurations, with addition given by $C_1 \oplus C_2 = \overline{C_1 + C_2}$. Here $+$ signifies the usual pointwise vector addition and $\overline{C_3}$ represents the unique critical configuration reachable from C_3. When v_0 is understood, we will abbreviate this group as the critical group of graph G, and denote it as $\mathcal{C}(G)$.

THEOREM 6. [**1**] $\mathcal{C}(G)$ *is in fact an abelian (associative) group.*

4. Connection to Elliptic Curves

We note an alternative definition of the critical group that gives it a form closer to the Picard group or Jacobian of an algebraic variety. Recall that divisors on elliptic curve E over $\mathbb{F}_q$ are formal integral linear combinations of points on $E(\overline{\mathbb{F}_p})$ which are invariant under Frobenius automorphism π which fixes finite field $\mathbb{F}_q$ ($q = p^k$). We consider relations of the form $D = \sum_i n_i P_i \sim 0$ whenever D is the divisor of a rational function. For an elliptic curve, this includes relations generated by those of the form $P + Q + R - 3P_\infty \sim 0$. Furthermore, for elliptic curves, the Abel-Jacobi map provides an isomorphism between the set of equivalence classes $[P - P_\infty]$ and the set of points $P \in E(\mathbb{F}_q)$. We thus encode all of these relations as a matrix, L_0, and then the Picard group or Jacobian of the Elliptic Curve is given as $\mathbb{Z}^{\#E(\mathbb{F}_q)} \Big/ \text{Im } L_0$.

Returning to the theory of chip-firing games, the literature for this subject occasionally uses the terms Picard group or Jacobian for the critical group as well. Let $\mathbb{Z}^{\#V}$ be the set of divisors on the set of vertices V. That is, we consider formal integral (possibly negative) linear combinations of v_1 through $v_{\#V}$. Alternatively we can think of these as the set of homomorphisms from V to $\mathbb{Z}$ or integral vectors of length $\#V$. Let L represent the Laplacian matrix for directed graph G, that is $L_{ii} = d(v_i)$ and $L_{i,j} = -d(v_i, v_j)$. The Laplacian will be a singular matrix with a nontrivial nullspace. However, if we take the minor which omits the row and column corresponding to v_0, then we get a nonsingular matrix L_0. The critical group of the graph (V, E) is isomorphic to $\mathbb{Z}^{\#V-1} \Big/ \text{Im } L_0$. Among other things, this implies by the Matrix-Tree Theorem that $|\mathcal{C}(G)|$ equals the number of spanning trees in G. Since $N_k = -\mathcal{W}_k(q, -N_1)$, we turn our attention to the critical group of the (q, t)-wheel graph for $q \geq 0$ and $t \geq 1$.

While it is easier to describe the group structure in terms of critical configuration vectors or as a cokernel, we do indeed have a bijection between spanning trees and critical configurations, and thus one could define the group structure directly on (colored) spanning trees.

THEOREM 7. *There exists an explicit* bijection *between critical configurations and spanning trees (at least in the case of the directed (q, t)-wheel multi-graph). This map induces an isomorphism of groups.*

Specifically pick one of the vertices on the rim to be v_1, and label v_2 through v_k clockwise. Label the central hub as v_0. For i between 1 and k, if $1 \leq C_i \leq q$, then fill in the arc between v_{i-1} and v_i, labeling it with the number C_i. (In the case of $i = 1$ we use the arc between v_k and v_1 instead.) If $1 + q \leq C_i \leq q + t$ then fill in the spoke between v_0 and v_i and label it with number C_i. After filling in the edges as indicated we will get a subgraph of a spanning tree. To complete this subgraph to a tree, fill in additional arcs using the

following rule: one may fill in an arc from v_{i-1} to v_i, and label it with a q, if and only if $C_i \in \{1+q, \ldots, q+t\}$. In other words, if $C_i = 0$ then this will contribute no arc nor a spoke.

PROOF. We defer the proof of this theorem until Section 5 where we precisely describe which critical configurations actually arise. It will then be clear that the list of configurations that show up as the image of a spanning tree, and the list of possible critical configurations, are equivalent. Since the described map is injective by construction, we have the desired bijection. □

4.1. Group Structure. We now return to the main topic at hand, namely elliptic curves. An elliptic curve over a finite field has a well-known group structure. In fact, it is the product of at most two cyclic groups. One way to prove this is by showing that for $gcd(N, p) = 1$, the $[N]$-torsion subgroup of $E(\overline{\mathbb{F}}_p)$ (also denoted as $E[N]$) is isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ and that $E[p^r]$ is either 0 or $\mathbb{Z}/p^r\mathbb{Z}$.

Since we know that the critical group of graphs are also abelian groups, this motivates the question: what is the group decomposition of the $\mathcal{C}(G)$'s? The case of a simple wheel graph W_k was explicitly found to be [**1**]

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

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 papers recently, e.g. [**3, 7**], and a common tool is the Smith normal form of the Laplacian. Fortunately, we already know the Smith normal form for the case we care about, namely for the (q, t)-wheel graphs. Using Theorem 3, (in fact Proposition 1 is sufficient), we show

THEOREM 8. *$\mathcal{C}(W_k(q, N_1))$ is isomorphic to at most two cyclic groups, a property that this sequence of critical groups shares with the family of elliptic curve groups over finite fields.*

In addition to a presentation for $\mathcal{C}(W_k(q, N_1))$, we also get a more explicit presentation of $E(\mathbb{F}_{q^k})$ in certain cases.

THEOREM 9. *If $E(\mathbb{F}_q) \cong \mathbb{Z}/N_1\mathbb{Z}$, as opposed to the product of two cyclic groups, and $End(E) \cong \mathbb{Z}[\pi]$, then*

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

for all $k \geq 1$. That is, $E(\mathbb{F}_{q^k})$ is the cokernel of the image of M_k. 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 we can take $\mathbb{Z}^k$ as being generated by $\{P, \pi(P), \ldots, \pi^{k-1}(P)\}$ under this presentation.

PROOF. A theorem of Lenstra [**5**] says that an **ordinary** elliptic curve over $\mathbb{F}_q$ has a group structure in terms of its endomorphism ring, namely,

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

Wittman [**17**] gives an explicit description of the possibilities for $End(E)$, given q and $E(\mathbb{F}_q)$. It is well known, e.g. [**11**], that the endomorphism ring in the ordinary case is an order in an imaginary quadratic field. This means that

$$End(E) \cong \mathcal{O}_g = \mathbb{Z} \oplus g\delta\mathbb{Z}$$

for some $g \in \mathbb{Z}_{\geq 0}$ and $\delta = \sqrt{D}$ or $\frac{1+\sqrt{D}}{2}$ according to d's residue modulo 4. Wittman shows that for a curve E with conductor f, the possible g's that occur satisfy $g|f$ as well as

$$n_1 = \gcd(a - 1, g/f).$$

The conductor f and constant a are computed by rewriting the Frobenius map as $\pi = a + f\delta$, and n_1 is the unique positive integer such that $E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ $(n_1|n_2)$.

We focus here on the case when $g = f$ and $End(E) \cong \mathbb{Z}[\pi]$. In particular, n_1 must be equal to one in this case, and so the condition that $End(E) = \mathbb{Z}[\pi]$ is actually a sufficient hypothesis. Since $E(\mathbb{F}_{q^k}) \cong \mathbb{Z}[\pi]/(1 - \pi^k)$ in this case, we get

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

with x transcendent over $\mathbb{Q}$. Thus

$$E(\mathbb{F}_{q^k}) \cong \mathbb{Z}\{1, x, x^2, \ldots, x^{k-1}\} \Big/ \Big(x^2 - (1+q-N_1)x + q,\ x^3 - (1+q-N_1)x^2 + qx,\ \ldots,\ x^{k-1} - (1+q-N_1)x^{k-2} + qx^{k-3},$$
$$1 - (1+q-N_1)x^{k-1} + qx^{k-2},\ x - (1+q-N_1) + qx^{k-1} \Big)$$

and using matrix M_k, as defined above, we obtain the desired presentation for $E(\mathbb{F}_{q^k})$ in this case. □

QUESTION 1. *What can we say in the case of another endomorphism ring, or the case when $E(\mathbb{F}_q)$ is not cyclic?*

4.2. Analogues of Elliptic Cyclotomic polynomials. We found for elliptic curves that $ECyc_d(q, N_1)$ counted the number of points in the kernel of the isogeny $Cyc_d(\pi)$ where π is the Frobenius isogeny. Since

$$N_k = \prod_{d|k} ECyc_d(q, N_1)$$

and $\mathcal{W}_k(q,t) = -N_k\Big|_{N_1 \to -t}$, it also makes sense to consider the decomposition

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

where $WCyc_d(q,t) = -ECyc_d|_{N_1 \to -t}$. A few of the first several $WCyc_d(q,t)$'s are given below:

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

We ask the same question as before, namely does there exist a combinatorial or geometric interpretation of these polynomials. Indeed, we consider the following properties of the $\mathcal{C}(W_k(q,t))$'s that allow us to derive an analogous result.

PROPOSITION 3. *The identity map is an injective group homomorphism between $\mathcal{C}(W_{k_1}(q,t))$ and $\mathcal{C}(W_{k_2}(q,t))$ whenever $k_1|k_2$. More precisely, we let $\mathcal{C}(W_{k_1}(q,t))$ embed into $\mathcal{C}(W_{k_2}(q,t))$ by letting $w \in \mathcal{C}(W_{k_1}(q,t))$ map to the word $www\ldots w \in \mathcal{C}(W_{k_2}(q,t))$ using $\frac{k_2}{k_1}$ copies of w.*

Define ρ to be the rotation map on $\mathcal{C}(W_k(q,t))$. If we consider elements of the critical group to be configuration vectors, then we mean circular rotation of the elements to the right. On the other hand, ρ acts by rotating the rim vertices of W_k clockwise if we view elements of $\mathcal{C}(W_k(q,t))$ as spanning trees.

PROPOSITION 4. *The kernel of $(1-\rho^{k_1})$ acting on $\mathcal{C}(W_{k_2}(q,t))$ is subgroup $\mathcal{C}(W_{k_1}(q,t))$ whenever $k_1|k_2$.*

We therefore can define a direct limit

$$\mathcal{C}(\overline{W}(q,t)) \cong \bigcup_{k=1}^{\infty} \mathcal{C}(W_k(q,t))$$

where ρ provides the transition maps.

Another view of $\mathcal{C}(\overline{W}(q,t))$ is as the set of bi-infinite words which are (1) periodic, and (2) have fundamental subword equal to a configuration vector in $\mathcal{C}(W_k(q,t))$ for some $k \geq 1$. In this interpretation, map ρ acts on $\mathcal{C}(\overline{W}(q,t))$ also. In this case, ρ is the shift map, and in particular we obtain

$$\mathcal{C}(W_k(q,t)) \cong Ker(1-\rho^k) : \mathcal{C}(\overline{W}(q,t)) \to \mathcal{C}(\overline{W}(q,t)).$$

We now can describe our variant of Theorem 4.

THEOREM 10.

$$WCyc_d = \left| Ker\Big(Cyc_d(\rho)\Big) : \ \mathcal{C}(\overline{W}(q,t)) \to \mathcal{C}(\overline{W}(q,t)) \right|$$

where ρ denotes the shift map, and $\mathcal{C}(\overline{W}(q,t))$ is the direct limit of the sequence $\{\mathcal{C}(W_k(q,t))\}_{k=1}^{\infty}$.

PROOF. The proof is analogous to the elliptic curve case. Since the maps $Cyc_{d_1}(\rho)$ and $Cyc_{d_2}(\rho)$ are group homomorphisms, we get

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

and the rest of the proof follows as in [**8**]. □

Thus we identify shift map ρ as being the analogue of the Frobenius map π on elliptic curves. In addition to ρ's appearance in Theorem 10, two other comparisons with π are highlighted below.

(1)

$$\begin{aligned} \mathcal{C}(W_k(q,t)) &\cong Ker(1-\rho^k) : \mathcal{C}(\overline{W}(q,t)) \to \mathcal{C}(\overline{W}(q,t)) \quad \text{just as} \\ E(\mathbb{F}_{q^k}) &= Ker(1-\pi^k) : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q). \end{aligned}$$

(2) We get the equation

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

which can be read off from matrix M_k and the configuration vectors' images under clockwise and counter-clockwise rotation. This is a simple analogue of the characteristic equation

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

of the Frobenius map π.

5. Characterization of Critical Configurations

In this section we completely characterize critical configurations of the (q,t)-Wheel graph. Furthermore, we will shortly see a deterministic finite automaton which admits such critical configurations. As an added bonus, we can construct a zeta function of such a system which is intimately connected to the zeta function of the elliptic curve.

This new characterization of critical configurations also proves Theorem 7, giving a bijection between critical configurations and spanning trees.

PROPOSITION 5. *A configuration $C = [c_1, c_2, \ldots, c_k]$ of the wheel graph $W_k(q,t)$ is stable if and only if $0 \leq c_i \leq q+t$ for all $1 \leq i \leq k$.*

PROOF. It is clear that we disallow $c_i < 0$ as a legal configuration by our definition. If such a configuration were to come up, we could add t to every value c_i, simulating the firing of the central vertex. If on the other hand, there exists $c_i \geq 1+q+t$, with all other $c_i \geq 0$, then vertex v_i can fire resulting in a new nonnegative configuration. Otherwise, if all c_i are in the specified range, we have a stable configuration where no vertex except the hub can fire. □

We recall that any stable configuration C is **critical** if and only if it is recurrent, meaning that after adding t to every c_i and applying the chip-firing rules, we arrive back at stable configuration C.

PROPOSITION 6. *There exists a unique critical configuration* reachable *from a given stable configuration.*

LEMMA 1. *Let C be a stable configuration, with $\sum_{i=1}^{k} c_i = N$. If C is reachable from some configuration C' (which is not necessarily stable) with $\sum_{i=1}^{k} c'_i > N$, then C is actually critical.*

PROOF. We need only check that if we add t to all values c_i and apply the chip-firing rules, we will reach C again. Given the sum of the rows of the Laplacian matrix, there will be some firing sequence such that every vertex will fire, and thus the result being the subtraction of t from every c_i, thus we obtain C again. See [**1**] for more details in the case of a general graph. □

LEMMA 2. *While we apply the chip-firing rules, every stage will decrease the $\sum_{i=1}^{k} c_i$ by t. In particular, if there are two stable configurations which are equivalent, we will reach the configuration with the biggest $\sum_{i=1}^{k} c_i$ first. Thus, this vector will be the critical configuration out of this equivalence class.*

PROOF. This claim follows from the definition of the Laplacian and Lemma 1. □

Thus we have proven Proposition 6 for the case of the (q,t)-wheel graph. For a more general proof, see [**1**].

LEMMA 3. *Any critical configuration $[c_1,\dots,c_k]$ will have at least one element $c_i = B$ such that $B \in \{1+q,\dots,q+t\}$.*

PROOF. Assume otherwise. Then $c_i \in \{0,1,\dots,q\}$ for all $1 \le i \le k$. Consequently, we may add t to every c_i and still obtain a stable configuration. Thus the initial configuration is smaller and cannot be critical. □

THEOREM 11. *Any configuration C is critical if and only if it consists of a circular concatenation of blokcs of the form*

$$B, M_1, \dots, M_j, 0, q, q, \dots, q$$

where $B \in \{1+q,\dots,q+t\}$ and $M_i \in \{1,\dots,q\}$.

PROOF. We have already shown that there exists at least one $c_i = B$ with $B > q$. Thus we prove this Theorem by induction on n, the number of such elements. Consider such a block in context, and presume it is of form

$$\cdots, M_n^{k_n} \mid B_1, M_1^1, M_1^2, \dots, M_1^{k_1} \mid B_2, \cdots$$

where $M_p^i \in \{0,1,\dots,q\}$ and $B_p \in \{1+q,\dots,q+t\}$. Here $M_n^{k_n}$ and B_2 represent the end of the previous block and the beginning of the next block, respectively. The heart of the proof is the verification of the following claim.

CLAIM 1. *Such a configuration cannot be recurrent unless $M_p^{j_p} = 0$ implies that the remaining M_p^i's, i.e. $M_p^{j_p+1}$ through $M_p^{k_p}$, are equal to q.*

Without loss of generality, we will work with $p = 1$ and let $j_1 = j$, $k_1 = k$, $M_n^{k_n} = M_0$. Assume that M_1^1 through $M_1^{j-1} \in \{1,2,\dots q\}$. We add t to every element of C, getting $C + [t]$, and then reduce via the chip-firing rules whenever we encounter an element with value greater or equal to $1+q+t$. Configuration $C+[t]$ contains element $B_1 + t$, with value $\ge 1+q+t$, but all other elements of the block are $< 1+q+t$. Once we replace $B_1 + t$ with $B_1 - 1 - q$, and its neighbors with $M_0 + t + 1$ and $M_1^1 + q + t$, respectively, we reduce $M_1^1 + q + t$ since its entry is now $\ge 1+q+t$. We continue inductively until we reach $M_1^j + q + t$ which is less than $1+q+t$ since $M_1^j = 0$ by assumption. At this point, the block looks like

$$M_0 + t + 1 \mid B_1 - q, M_1^1, \dots, M_1^{j-1} - 1, q + t, M_1^{j+1} + t, \dots, M_1^k + t \mid B_2 + t.$$

Since $B_2 + t \ge 1 + q + t$, we can reduce this block further as

$$M^0 + t + 1 \mid B_1 - q, M_1^1, \dots, M_1^{j-1} - 1, q + t, M_1^{j+1} + t, \dots, M_1^k + t + 1 \mid B_2 - 1 - q.$$

By propagating the same reductions to the rest of the configuration, we reduce to a configuration C' which is made up of blocks of the form

$$B_p - q, M_p^1, \dots, M_p^{j_p-1} - 1, q + t, M_p^{j_p+1} + t, \dots, M_p^{k_p} + t + 1$$

in lieau of

$$B_p, M_p^1, \dots, M_p^{j_p-1}, 0, M^{j_p+1}, \dots, M^{k_p}.$$

Since $M_p^i \le q$, all elements of C' are less than $1+q+t$ except possibly for the last elements of each block, e.g. $M_p^k + t + 1$. If all of the M_p^k's are less than q, then C' is stable, and thus the original configuration C is not recurrent, nor critical as assumed.

Thus, without loss of generality, assume that $M_1^k = q$. We then can reduce block

$$M^0 + t + 1 \mid B_1 - q, M_1^1, \ldots, M_1^{j-1} - 1, q + t, M_1^{j+1} + t, M_1^{j+2} + t \ldots, M_1^{k-1} + t, q + t + 1 \mid B_2 - 1 - q$$

and obtain

$$M^0 + t + 1 \mid B_1 - q, M_1^1, \ldots, M_1^{j-1} - 1, q + t, M_1^{j+1} + t, M_1^{j+2} + t \ldots, M_1^{k-1} + t + 1, 0 \mid B_2 - 1.$$

By analogous logic, we must have that $M_1^{k-1} = q$ and continuing iteratively, we reduce to

$$M^0 + t + 1 \mid B_1 - q, M_1^1, \ldots, M_1^{j-1} - 1, q + t + 1, 0, q, \ldots, q, q \mid B_2 - 1$$

which is equivalent to

$$M^0 + t + 1 \mid B_1 - q, M_1^1, \ldots, M_1^{j-1}, 0, q, q, \ldots, q, q \mid B_2 - 1.$$

Finally, $M^0 = M_n^{k_n}$ so we indeed obtain

$$q \mid B_1, M_1^1, \ldots, M_1^{j-1}, 0, q, q, \ldots, q, q \mid B_2$$

after iterating over all the blocks to the right and wrapping around.

□

6. Connections to Deterministic Finite Automata

A deterministic finite automaton (DFA) is a finite state machine M built to recognize a given language L, i.e. a set of words in a specific alphabet. To test whether a given word ω is in language L we write down ω on a strip of tape and feed it into M one letter at a time. Depending on which state the machine is in, it will either accept or reject the character. If the character is accepted, then the machine's next state is determined by the previous state and the relevant character on the strip. As the machine changes states accordingly, and the entire word is fed into the machine, if all letters of ω are accepted, then ω is an element of language L.

For our purposes we consider an automaton M_G with three states, which we label as A, B, and C. In state A we either accept a character in $\{1+q, \ldots, q+t\}$ and return to state A, accept a character in $\{1, \ldots, q\}$ and move to state B, or accept the character 0 and move to state C.

On the other hand, in state B we either accept a character in $\{1 + q, \ldots, q + t\}$ and move to state A, accept a character in $\{1, \ldots, q\}$ and return to state B, or accept character 0 and move to state C.

Finally, in state C we either accept a character in $\{1 + q, \ldots, q + t\}$ and move to state A, or accept character q and return to state C. A character in $\{1, \ldots, q\}$ is not accepted while in state C.

If we consider the set of words which are accepted by M_G with the properties (1) the initial state of M_G is the same as its final state, and (2) M_G is in state A at some point while verifying ω, then the language that we obtain are precisely the set of critical configurations, as described in Section 5. Using terminology of [**10**], the set of critical configurations of (q, t)-W_k is given as the set of words which are the trace of M_G *minus* the trace of cycles only containing state B *minus* the trace of cycles only containing state C. We note that all other circuits with the same initial and final state necessarily need to contain state A since there are no cycles containing both state B and C but not A. There is no way to go from state C to state B without going through state A first, given the definition of M_G. Thus the zeta function of this cyclic language is given as

$$\frac{\det([1 - qT]) \det([1 - T])}{\det(I - MT)}$$

where the factor of $\det([1 - qT])$ correspond to the trace of cycles containing state B alone, and $\det([1 - T])$ corresponds to the trace of cycles containing state C alone. On the other hand, matrix M is the 3-by-3 matrix encoded by the number of directed edges between the various states.

$$\begin{bmatrix} t & q & 1 \\ t & q & 1 \\ t & 0 & 1 \end{bmatrix}$$

Thus

$$\exp\left(\sum_{k=1}^{\infty} \frac{\mathcal{W}_k}{k} T^k\right) = \frac{(1 - qT)(1 - T)}{1 - (1 + q + \mathcal{W}_1)T + qT^2}$$

where $\mathcal{W}_k$ equals the number of primitive cycles in M_G, which contain state A but starting at any of the three states.

At this point, we have yet a fourth proof of the Theorem 1, which states $N_k = -\mathcal{W}_k(q, -N_1)$. The reasoning being

$$\begin{aligned}
\exp\left(\sum_{k\geq 1}\frac{\mathcal{W}_k}{k}T^k\right) &= \frac{(1-qT)(1-T)}{1-(1+q+t)T+qT^2} \\
&= \left(\frac{1-(1+q+t)T+qT^2}{(1-qT)(1-T)}\right)^{-1} \\
&= (Z(E,T)|_{N_1=-t})^{-1} \\
&= \exp\left(-\sum_{k\geq 1}\frac{N_k}{k}T^k\right)\Big|_{N_1=-t}.
\end{aligned}$$

The relationship between elliptic curves and spanning trees appears even more pronounced than one would have guessed from the motivation of Theorem 1. The connections described here inspire further exploration for connections between these two families of objects. This work includes the search for a natural bijection between the set of points on an elliptic curve, and a certain subset of the spanning trees of the (q,t)-wheel graphs, as well as for combinatorial interpretations of the coefficients in the $WCyc_d$'s.

References

[1] N. L. Biggs, Chip-Firing and the Critical Group of a Graph. Journal of Algebraic Combinatorics. **9** (1999), 22-45.

[2] A. Garsia and G. Musiker, *Basics on Hyperelliptic Curves over Finite Fields*, in progress.

[3] B. Jacobson, A. Neidermaier, V. Reiner, Critical groups for complete multipartite graphs and Cartesian products of complete graphs. (2002), `http://www.math.umn.edu/~reiner/Papers/papers.html`

[4] M. Latapy and H. Pham, The lattice structure of chip firing games and related models. *Phys. D*, **155(1-2)** (2001), 69-82.

[5] H. W. Lenstra, Complex Multiplication Structure of Elliptic Curves. Journal of Number Theory. **56** (1996), 227-241.

[6] N. Loehr, G. Warrington, and H. Wilf, The combinatorics of a three-line circulant determinant. *Israel J. Math.*, **143** (2004), 141–156.

[7] M. Maxwell. Enumerating Bases of Self-Dual Matroids. (2006), `http://garsia/math.yorku.ca/fpsac06/papers73.pdf`

[8] G. Musiker, Combinatorial Aspects of Elliptic Curves. (submitted)

[9] C. Reutenauer, $\mathbb{N}$-Rationality of zeta functions. Advances in Applied Mathematics. **18** (1997), 1-17.

[10] C. Reutenauer and J. Berstel. Zeta functions of formal languages. Transactions of the American Mathematical Society, Vol. 321, No. 2, (Oct., 1990), 533-546.

[11] J. Silverman. *The arithmetic of elliptic curves, volume* 106 *of Graduate Texts in Mathematics*, Springer-Verlag, New York (1986).

[12] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences/index.html`.

[13] R. P. Stanley, *Enumerative Combinatorics Vol. 2, volume 62 of Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge (1999).

[14] D.G. Wagner, The critical group of a direct graph. `arXiv:math.CO/0010241`.

[15] L. Washington. *Elliptic curves: Number theory and cryptography. Discrete Mathematics and its Applications*, Chapman & Hall/CRC, Boca Raton, (2003).

[16] A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann, Paris (1948).

[17] C. Wittman. Group Structure of elliptic curves over finite fields. J. of Number Theory **88** (2001), 335-344.

DEPARTMENT OF MATHEMATICS, UCSD, SAN DIEGO, USA, 92093-0112

E-mail address: `gmusiker@math.ucsd.edu`