DISCRETE LOGARITHM ON THE JACOBIAN OF FINITE GRAPHS

FARBOD SHOKRIEH

Abstract. Every graph has a canonical finite abelian group attached to it. This group has appeared in the literature under a variety of names including the sandpile group, critical group, Jacobian group, and Picard group. The construction of this group closely mirrors the construction of the Jacobian variety of an algebraic curve. Motivated by this analogy, it was recently suggested by Norman Biggs that the critical group of a finite graph is a good candidate for doing discrete logarithm based cryptography. In this paper, we study a bilinear pairing on this group and show how to compute it. Then we use this pairing to find the discrete logarithm efficiently, thus showing that the associated cryptographic schemes are not secure. Our approach resembles the MOV attack on elliptic curves.

1. Introduction

1.1. Overview. Every graph has a canonical finite abelian group whose order is the number of spanning trees of the graph. This group has appeared in the literature under many different names; in theoretical physics it was first introduced as the “abelian sandpile group” or “abelian avalanche group” in the context of self-organized critical phenomena ([3, 16, 19]). In arithmetic geometry, this group appeared as the “group of components” in the study of degenerating algebraic curves ([20]). In algebraic graph theory this group appeared under the name “Jacobian group” or “Picard group” in the study of flows and cuts in graphs ([2]). The study of a certain chip-firing game on graphs led to the definition of this group under the name “critical group” ([8, 9]).

The construction of this group closely mirrors the construction of the Jacobian variety of an algebraic curve. Motivated by this analogy, Norman Biggs in [10] suggests that the Jacobian of a finite graph (which he calls the “critical group”) might be suitable for discrete logarithm based cryptography.

In this paper, we study the discrete logarithm problem on the Jacobian of finite graphs. Our main result is an algorithm to efficiently compute discrete logarithms on these groups. Therefore, unlike elliptic curves and Jacobian varieties, one can not use the Jacobian of finite graphs for cryptographic purposes. It is an intriguing problem

Date: April 8, 2009.

2000 Mathematics Subject Classification. 05C50, 14H40, 11Y99.

I would like to thank Matthew Baker for recommending this problem to me, and for many helpful discussions. Thanks also to Richard Lipton, Dino Lorenzini, and Prasad Tetali for their helpful comments.
whether the fact that discrete logarithm can be done efficiently might have any algorithmic applications. Our algorithm uses a bilinear pairing, which we call the monodromy pairing, on this group. This approach is similar to the MOV attack on elliptic curves. For our application, we study the monodromy pairing and show how to compute it.

1.2. Related work. The order of the Jacobian group is the number of spanning trees of the graph [8]. Hence, the order of the group can be computed by the famous matrix-tree formula of Kirchhoff.

Finite graphs and algebraic curves behave similarly in many respects. Recently, there have been an increasing number of papers pursuing this analogy. Some relationship between elliptic curves and chip-firing games on graphs is noticed in [24]. In [5, 4] a version of the famous Riemann-Roch theorem is proved for finite graphs, a discrete analogue of holomorphic maps between Riemann surfaces is introduced, and a graph-theoretic Riemann-Hurwitz formula is proved. A Torelli’s theorem for graphs is proved in [1, 14]. The relationship between graph theory and algebraic geometry goes beyond a simple analogy. For example, Mikhalkin and Zharkov in [23] prove that an (abstract) “tropical curve” is simply a connected “metric graph”.

1.3. Previous work. Norman Biggs in [10] constructs a family of graphs with cyclic Jacobian groups, to be potentially used for cryptography. The problem of finding families of graphs with cyclic Jacobian groups is subsequently studied in [21, 15, 24]. These provide examples of cyclic Jacobian groups with appropriate order, so that discrete logarithm problem cannot be solved by the known purely group theoretic methods.

After completion of our work, we discovered a preprint by Blackburn ([11]) in which the discrete logarithm problem is addressed for the particular family of graphs constructed by Biggs in [10]. It is fairly clear that methods presented in [11], with some minor modifications, can also be applied to the general case. Our method is quite different from Blackburn’s method, and our algorithm in [4] also works for any graph with a cyclic Jacobian group.

To our knowledge, the monodromy pairing was first introduced by Bosch and Lorenzini in [13]. We have not found an easy-to-compute formula, like (3.9), in the literature.

The paper proceeds as follows. In §2 we provide the relevant definitions. The monodromy pairing is studied in §3. Using the monodromy pairing, we give our discrete logarithm algorithm in §4. Further remarks and results are outlined in §5. Appendix A contains a new proof of Theorem 3.5.

2. Definitions

2.1. Notation and Terminology. Throughout this paper, a graph means a finite, unweighted multigraph with no loops. All graphs are assumed to be connected. For a graph $G$, the set of vertices is denoted by $V(G)$, and the set of edges is denoted
by \( E(G) \). Throughout this paper, \( n \) and \( m \) denote the number of vertices and edges, respectively.

Let \( \{ v_1, \ldots, v_n \} \) be an ordering of \( V(G) \). With respect to this ordering, the *Laplacian matrix* \( Q \) associated to \( G \) is the \( n \times n \) matrix \( Q = (q_{ij}) \), where \( q_{ii} \) is the degree of vertex \( v_i \), and \( -q_{ij} \) (\( i \neq j \)) is the number of edges connecting \( v_i \) and \( v_j \). It is well-known (and easy to verify) that \( Q \) is symmetric, has rank \( n - 1 \), and the kernel of \( Q \) is spanned by \( 1 \), the all-one vector (see, e.g., [7, 12]).

2.2. The Jacobian of a finite graph. Let \( \text{Div}(G) \) be the free abelian group generated by \( V(G) \). One can think of elements of \( \text{Div}(G) \) as formal integer linear combination of vertices

\[
\text{Div}(G) = \left\{ \sum_{v \in V(G)} a_v(v) : a_v \in \mathbb{Z} \right\}.
\]

By analogy with the algebraic curve case, elements of \( \text{Div}(G) \) are called *divisors* on \( G \). For a divisor \( D \), the coefficient \( a_v \) of \( (v) \) in \( D \) is denoted by \( D(v) \).

We define by \( \mathcal{M}(G) = \text{Hom}(V(G), \mathbb{Z}) \) the abelian group consisting of all integer-valued functions on the vertices. One can think of \( \mathcal{M}(G) \) as analogous to the group \( \mathcal{M}(X)^\times \) of nonzero meromorphic functions on an algebraic curve \( X \).

For \( f \in \mathcal{M}(G) \), \( \text{div}(f) \in \text{Div}(G) \) is given by the formula

\[
\text{div}(f) = \sum_{v \in V(G)} \text{ord}_v(f)(v),
\]

where

\[
\text{ord}_v(f) = \sum_{\{v,w\} \in E(G)} (f(v) - f(w)).
\]

Consider the group homomorphism \( \text{deg} : \text{Div}(G) \to \mathbb{Z} \) defined by \( \text{deg}(D) = \sum_{v \in V(G)} D(v) \).

Denote by \( \text{Div}^0(G) \) the kernel of this homomorphism, consisting of *divisors of degree zero*. Define \( \text{Prin}(G) = \{ \text{div}(f) \in \text{Div}(G) : f \in \mathcal{M}(G) \} \) to be the group of *principal divisors*.

**Lemma 2.1.** \( \text{Prin}(G) \subseteq \text{Div}^0(G) \), and both \( \text{Prin}(G) \) and \( \text{Div}^0(G) \) are free \( \mathbb{Z} \)-modules of rank \( n - 1 \).

A proof is given in [8]. As a corollary, the quotient group

\[
\text{Jac}(G) = \text{Div}^0(G) / \text{Prin}(G)
\]

is well-defined and is a finite abelian group. Following [2], it is called the *Jacobian* or the *Picard*\(^2\) group of \( G \).

**Lemma 2.2.** \([2, 8]\) The order of the group \( \text{Jac}(G) \) is equal to the number of spanning trees in \( G \), which we denote by \( \kappa(G) \).

\(^1\)Remember that \( G \) has no loops.

\(^2\)Another appropriate notation is \( \text{Pic}^0(G) \).
Following \cite{5}, for \(D_1, D_2 \in \text{Div}(G)\), we say that \(D_1\) is equivalent to \(D_2\), and write \(D_1 \sim D_2\), if \(D_1 - D_2\) is a principal divisor.

3. **A bilinear pairing on the Jacobian of finite graphs**

3.1. **Generalized inverses.** A matrix can have an inverse only if it is square and its columns (or rows) are linearly independent. But one can still get “partial inverse” of any matrix.

**Definition.** Let \(A\) be a matrix (not necessarily square). Any matrix \(L\) satisfying \(ALA = A\) is called a generalized inverse of \(A\).

It is somehow surprising that for every matrix \(A\) there exists at least one generalized inverse. In fact, more is true; every matrix has a unique Moore-Penrose pseudoinverse\[^4\].

Let \(Q\) be the Laplacian matrix of a connected graph. Since its rank is \(n - 1\), it cannot have an inverse. But there are many ways to obtain generalized inverses:

**Example 3.1.** Fix an integer \(1 \leq i \leq n\). Let \(Q_i\) be the \((n - 1) \times (n - 1)\) matrix obtained from \(Q\) by deleting \(i\)th row and \(i\)th column. Then \(Q_i\) is a full rank matrix and has an inverse \(Q_i^{-1}\). Let \(L(i)\) be the \(n \times n\) matrix obtained from \(Q_i^{-1}\) by inserting a zero row after the \((i - 1)\)th row and inserting a zero column after the \((i - 1)\)th column. Then \(L(i)\) is a generalized inverse of \(Q\). One can check that

\[
QL(i) = I + R(i),
\]

where \(I\) is the identity matrix, and \(R(i)\) has \(-1\) entries in the \(i\)th row and is zero everywhere else. As \(R(i)Q = 0\), we get \(QL(i)Q = Q\).

**Example 3.2.** Let \(J\) be the \(n \times n\) all-one matrix. Then \(Q + \frac{1}{n}J\) is nonsingular and \(Q^+ = (Q + \frac{1}{n}J)^{-1} - \frac{1}{n}J\) is a generalized inverse of \(Q\). In fact it is the unique Moore-Penrose pseudoinverse of \(Q\); it is easy to check \(QQ^+ = Q^+Q = I - \frac{1}{n}J\) and \(Q^+QQ^+ = Q^+\).

These examples show that computing a generalized inverse \(L\) takes time at most \(O(n^\omega)\), where \(\omega\) is the exponent for matrix multiplication.

3.2. **The monodromy pairing.** A kind of graph-theoretic analogue of Weil pairing on the (principally polarized) Jacobian of an algebraic curve is provided by a certain bilinear pairing on \(\text{Jac}(G)\), which we define in this section\[^4\].

For \(D_1, D_2\) in \(\text{Div}^0(G)\), let \(m_1\) and \(m_2\) be integers such that \(m_1D_1 = \text{div}(f_1)\) and \(m_2D_2 = \text{div}(f_2)\) are principal; these exist because \(\text{Jac}(G)\) is a finite group. One can easily show that

\[
\frac{1}{m_2} \sum_{v \in V(G)} D_1(v)f_2(v) = \frac{1}{m_1} \sum_{v \in V(G)} f_1(v)D_2(v).
\]

\[^3\]The Moore-Penrose pseudoinverse of \(A\) is a generalized inverse of \(A\) with three extra properties; see \cite{6} for an extensive study of the subject.

\[^4\]The monodromy pairing is symmetric, while the Weil pairing is skew-symmetric.
The pairing \( \langle \cdot, \cdot \rangle : \text{Div}^0(G) \times \text{Div}^0(G) \to \mathbb{Q} \) defined by
\[
\langle D_1, D_2 \rangle = \frac{1}{m_2} \sum_{v \in V(G)} D_1(v) f_2(v)
\]
is symmetric and bilinear. This pairing descends to a well-defined pairing on \( \text{Jac}(G) \). We use the notation \( \overline{D} \) for an element of \( \text{Jac}(G) \), if \( D \) is a lift of that element in \( \text{Div}^0(G) \).

**Theorem 3.5.** The pairing \( \langle \cdot, \cdot \rangle : \text{Jac}(G) \times \text{Jac}(G) \to \mathbb{Q}/\mathbb{Z} \) defined by
\[
\langle \overline{D}_1, \overline{D}_2 \rangle = \frac{1}{m_2} \sum_{v \in V(G)} D_1(v) f_2(v) \pmod{\mathbb{Z}},
\]
where \( m_2 D_2 = \text{div}(f_2) \), is a well-defined, symmetric, bilinear, non-degenerate pairing on \( \text{Jac}(G) \).

This theorem, in a slightly different language, is proved in [13]. We give a more elementary proof in Appendix A.

**Definition.** We call the pairing described in Theorem 3.5 the **monodromy pairing** (see remark 1 in §5 for this terminology).

**Remark 3.7.** Let \( \Phi \) be a finitely generated abelian group. A symmetric bilinear pairing \( \langle \cdot, \cdot \rangle : \Phi \times \Phi \to \mathbb{Q}/\mathbb{Z} \) is called **non-degenerate** (or regular) if the group homomorphism \( \Phi \to \text{Hom}_\mathbb{Z}(\Phi, \mathbb{Q}/\mathbb{Z}) \) defined by \( x \mapsto (x, \cdot) \) is injective. If it is an isomorphism, it is called **perfect** (or unimodular). If a pairing on a finitely generated abelian group is non-degenerate, then it is automatically perfect\(^5\) (see [18]). For a finite abelian group \( \Phi \), this fact is immediate; there exists a (non-canonical) isomorphism between \( \Phi \) and its Pontryagin dual \( \text{Hom}_\mathbb{Z}(\Phi, \mathbb{Q}/\mathbb{Z}) \) (see p. 167 of [17]).

Let \( \{v_1, \ldots, v_n\} \) be an ordering of \( V(G) \). Let \( Q \) be the Laplacian matrix with respect to this ordering. This ordering gives an isomorphism between abelian groups \( \text{Div}(G) \), \( \mathcal{M}(G) \), and the \( \mathbb{Z} \)-module of \( n \times 1 \) column vectors having integer coordinates. Let \( [D] \) denote the column vector corresponding to \( D \in \text{Div}(G) \), and \( [f] \) denote the column vector corresponding to \( f \in \mathcal{M}(G) \).

The given definition of the monodromy pairing in (3.6) is canonical. However, the following proposition simplifies the proof of Theorem 3.5. Moreover, it shows how one can compute the monodromy pairing in practice.

**Proposition 3.8.** Let \( L \) be any generalized inverse of the Laplacian matrix \( Q \). Then the monodromy pairing is given by
\[
\langle \overline{D}_1, \overline{D}_2 \rangle = [D_1]^T L [D_2] \pmod{\mathbb{Z}}.
\]

\(^5\)Moreover, the group is torsion in this situation.
Proof. By definition $m_i[D_i] = [\text{div}(f_i)] = Q[f_i]$ for $i = 1, 2$. Result follows from the following computations. All equalities are mod $\mathbb{Z}$

\[
(D_1, D_2) = \frac{1}{m_2} \sum_{v \in V(G)} D_1(v)f_2(v)
= \frac{1}{m_2} [D_1]^T [f_2]
= \frac{1}{m_1 m_2} (Q[f_1])^T [f_2]
= \frac{1}{m_1 m_2} [f_1]^T Q[f_2]
= \frac{1}{m_1 m_2} [f_1]^T QLQ[f_2]
= \frac{1}{m_1 m_2} (Q[f_1])^T L(Q[f_2])
= [D_1]^T L[D_2] \pmod{\mathbb{Z}}.
\]

We emphasize that any generalized inverse of the Laplacian matrix can be used in (3.9).

4. Discrete Logarithm Problem on the Jacobian of a finite graph

Let $(\Phi, +)$ be a cyclic group. The Discrete Logarithm Problem (DLP) can be stated as:

Given $g, h \in \Phi$ with $x \cdot g = h$ for some integer $x$, compute $x \pmod{\text{ord}(g)}$.

In this section we use the monodromy pairing to solve the DLP for the Jacobian of a finite graph $G$ when $\text{Jac}(G)$ is cyclic.

In our context, we assume the elements of $\text{Jac}(G)$ are presented by some (arbitrary) lifts in $\text{Div}^0(G)$. Also, we assume a generator $g$ of the cyclic group $\text{Jac}(G)$ is known. We can compute and save a generalized inverse $L$ of $Q$ as outlined in §3.1.

Algorithm. (DLP on $\text{Jac}(G)$)

Input: $D, D' \in \text{Div}^0(G)$ such that $D' = x \cdot D$ in $\text{Jac}(G)$

Output: $x \pmod{\text{ord}(D)}$, the order of $D \in \text{Jac}(G)$.

1. Compute $(D, g) = r + \mathbb{Z}$ and $(D', g) = r' + \mathbb{Z}$ using formula (3.9).
2. Solve the Diophantine equation $r' = rx + y$ (for variables $x, y \in \mathbb{Z}$) by clearing the denominators of $r$ and $r'$ and using the extended Euclidean algorithm, to get $x \pmod{\text{ord}(D)}$.

\footnote{There are several efficient methods to find a generator; we omit the details here.}
Analysis of the algorithm. Since the monodromy pairing is bilinear, we have 
\((\overline{D'}, g) = x(\overline{D}, g)\), or \(r' = rx\) in \(Q/\mathbb{Z}\). We still need to prove that solving the Diophantine equation precisely gives \(x\) modulo the order of \(\overline{D}\) in Jac\((G)\).

Lemma 4.1. Let \(g\) be a generator of the cyclic group Jac\((G)\). Let \(h\) be any element of Jac\((G)\). If \(\langle h, g \rangle = \frac{a}{b} + \mathbb{Z} (a, b \in \mathbb{Z}, \gcd(a, b) = 1)\) then \(b\) is precisely the order of \(h\) in Jac\((G)\).

Proof. Let \(\gamma\) be the order of \(h\) in Jac\((G)\). By bilinearity of the monodromy pairing, 
\(\frac{\gamma a}{b} + \mathbb{Z} = \gamma \langle h, g \rangle = \langle \gamma \cdot h, g \rangle = \langle 0, g \rangle = \mathbb{Z}\), and therefore \(b | \gamma\).

On the other hand, \(\langle b \cdot h, g \rangle = b\langle h, g \rangle = a + \mathbb{Z} = \mathbb{Z}\). Since Jac\((G)\) is cyclic and the monodromy pairing is bilinear, all elements of Jac\((G)\) must pair trivially with \(b \cdot h\). By non-degeneracy of the monodromy pairing we get \(b \cdot h = 0\), which means \(\gamma | b\). Therefore \(\gamma = b\). \(\square\)

Now we can show that the algorithm precisely gives \(x\) mod the order of \(\overline{D}\) in Jac\((G)\); since \(\overline{D'} = x \overline{D}\), order of \(\overline{D'}\) divides the order of \(\overline{D}\). By Lemma 4.1, for \(r = \frac{a}{b}\) \((a, b \in \mathbb{Z}, \gcd(a, b) = 1)\), \(b\) is the order of \(\overline{D}\) in Jac\((G)\). Multiplying by \(b\) clears the denominators in \(r' = rx + y\), and we get \(ax + by = c\), for some integer \(c\). It is an elementary fact that the linear Diophantine equation \(ax + by = c\) (with \(\gcd(a, b) = 1\)) has solution, and \(x\) is determined mod \(b\).

Both steps (1) and (2) can be done in time at most \(O(n^2)\). \(\square\)

Remark 4.2 (DLP on the Critical group of finite graphs). Fix a vertex \(q\). In [10] each element of the Jacobian group is presented by a canonical (relative to the base vertex \(q\)) lift in Div\(^0\)(\(G\)), which is called the critical configuration (based at \(q\)), and is defined by a certain chip-firing game on the graph. It is known that in each equivalence class of divisors there is a unique such critical configuration. \(q\)-reduced divisors (or \(G\)-parking functions based at \(q\)) provide another set of canonical elements for equivalence classes (see, e.g., [27] and references therein). Hence, the group law on the Jac\((G) = \text{Div}^0(G)/\text{Prin}(G)\) induces a group law on the set of \(q\)-critical configurations, or the set of \(q\)-reduced divisors. Biggs ([9]) calls the former set with the induced group law the critical group \(K(G)\) of the graph, and suggests in [10] that the DLP is hard on the critical group. We note that the algorithm given in this paper works for any lift of elements of Jac\((G)\) to Div\(^0\)(\(G\)), and therefore it also solves the DLP on the critical group, as well as the “reduced divisors group”. Some related algorithmic questions are studied in [27] and [28].

5. Concluding remarks

We conclude with some remarks.

\(^7\)In particular, cardinality of these sets are equal to the number of spanning trees.
1. The pairing described in Theorem 3.5 is called the monodromy or Grothendieck’s pairing for the following reason. If $K$ is the field of fractions of a strictly henselian discrete valuation ring $R$, then a theorem of Raynaud [26] asserts that the component group $\Phi_J$ of the Néron model of the Jacobian $J$ of a semistable curve $X/K$ is isomorphic to the Jacobian of the dual graph $G$ of the special fiber of any semistable regular model for $X$ over $R$. Under the isomorphism provided by Raynaud’s theorem, the pairing on $\text{Jac}(G)$ which we described in §3.2 corresponds to Grothendieck’s monodromy pairing on $\Phi_J$ (see [13]).

2. By Abel’s theorem for graphs (see [2]), there is a canonical isomorphism

$$\text{Div}^0(G)/\text{Prin}(G) \cong H_1(G, \mathbb{Z})^\# / H_1(G, \mathbb{Z})$$

where $H_1(G, \mathbb{Z})^\#$ denotes the dual of the cycle lattice $H_1(G, \mathbb{Z})$ with respect to the standard inner product on the 1-chain group $C_1(G, \mathbb{Z})$. It can be shown that under this canonical isomorphism, the monodromy pairing on $\text{Div}^0(G)/\text{Prin}(G)$ corresponds to the negative of the discriminant form on $H_1(G, \mathbb{Z})^\# / H_1(G, \mathbb{Z})$. This and some relevant results will appear in a subsequent paper by the author.

3. Our approach to solve the DLP on the Jacobian of finite graphs resembles the MOV attack of Menezes, Okamoto, and Vanstone [22] for the DLP on elliptic curves. However, because the target group of the monodromy pairing is $\mathbb{Q}/\mathbb{Z}$ (instead of $\mathbb{F}_{q^\alpha}$), and because of Lemma 4.1, we get a deterministic polynomial-time solution for cyclic Jacobian (instead of a probabilistic polynomial-time reduction to the DLP in the group $\mathbb{F}_{q^\alpha}$).

4. If $\text{Jac}(G)$ is not cyclic, then one can still use the monodromy pairing, and solve the DLP efficiently. The idea is very similar to the MOV attack for elliptic curves; one can compute enough congruences for $x$ to eventually find $x \mod \text{ord}(D)$. We omit the details here.

5. We have found at least two other methods of solving the DLP in this context. One method is essentially applying the independent work of Blackburn ([11]) to arbitrary graphs. In our judgment, the solution presented in this paper is particularly nice, and there is no need to present the other approaches.

6. It is worth investigating how the given solution to the DLP for the Jacobian of finite graphs can relate to the DLP for the Jacobian of algebraic curves.

7. It is an intriguing problem whether the fact that discrete logarithm can be done efficiently might have any algorithmic applications. Also the fact that

---

8. If $\Lambda$ is an integral lattice (i.e., a free $\mathbb{Z}$-module of finite rank endowed with a non-degenerate $\mathbb{Z}$-valued symmetric bilinear form), then the dual lattice $\Lambda^\#$ contains $\Lambda$ as a finite index subgroup, and the quotient group $\Lambda^\#/\Lambda$ (called the discriminant group of the lattice) inherits in a natural way a non-degenerate $\mathbb{Q}/\mathbb{Z}$-valued symmetric bilinear form, called the discriminant form (see [24] for more details).

9. We also note that the monodromy pairing is symmetric, while the Weil pairing is skew-symmetric.
the Jacobian group is actually a bilinear group with an efficiently computable pairing might have other algorithmic applications.

**Appendix A. Proof of Theorem 3.5**

Here we outline an elementary proof of Theorem 3.5. We choose an ordering of $V(G)$ and use the formula (3.9).

*Pairing is bilinear.* This is obvious!

*Pairing is symmetric.* This follows from (3.3). Alternatively, if $L$ is any generalized inverse of $Q$ then $L^T$ is also a generalized inverse of $Q$ (because $Q$ is symmetric) and we have

$$
\langle D_2, D_1 \rangle = [D_2]^T L[D_1] \pmod{Z}
= ([D_1]^T L^T [D_2])^T \pmod{Z}
= [D_1]^T L^T [D_2] \pmod{Z}
= \langle D_1, D_2 \rangle.
$$

*Pairing is well-defined.* Let $D_2$ and $D'_2$ in $\text{Div}^0(G)$ be two different lifts of $\overline{D}_2 \in \text{Jac}(G)$. Then they differ by a principal divisor $[D'_2] = [D_2] + Q[g]$ for some $g \in \mathcal{M}(G)$. Let $m_1[D_1] = Q[f_1]$. Then

$$
[D_1]^T L[D'_2] = [D_1]^T L[D_2] + [D_1]^T LQ[g]
= [D_1]^T L[D_2] + \frac{1}{m_1}[f_1]^T QLQ[g]
= [D_1]^T L[D_2] + \frac{1}{m_1}[f_1]^T Q[g]
= [D_1]^T L[D_2] + [D_1]^T [g].
$$

So $[D_1]^T L[D'_2] = [D_1]^T L[D_2] \pmod{Z}$. By symmetry the same is true for different lifts of $D_1$.

*Pairing is non-degenerate.* We should show that if $D_1 \in \text{Div}^0(G)$ be such that

$$
\langle D_1, \cdot \rangle \equiv 0 \pmod{Z}
$$

then $D_1$ is a principal divisor. Let $x = L^T [D_1] \in \mathbb{Q}^n$. If $\langle \overline{D}, \cdot \rangle \equiv 0 \pmod{Z}$, then $x^T u \in \mathbb{Z}$, for any zero-sum column vector $u \in \mathbb{Z}^n$. Substituting $e_i - e_1$ for $u$ (where $e_i$ denotes the vector with a 1 in the $i^{th}$ coordinate and 0’s elsewhere), we get $x = r \mathbf{1} + v$ for some $r \in \mathbb{Q}$ and $v \in \mathbb{Z}^n$ ($\mathbf{1}$ denotes the all-one vector). Multiplying by $Q$, we have $Qx = rQ \mathbf{1} + Qv = Qv$ or $QL^T [D_1] = Qv$. Using $m_1[D_1] = Q[f_1]$ and the fact that $L^T$
is also a generalized inverse of $Q$, we get

$$QL^T[D_1] = \frac{1}{m_1}QL^TQ[f_1]$$

$$= \frac{1}{m_1}Q[f_1]$$

$$= [D_1].$$

Therefore we have shown $[D_1] = Qv$ for some $v \in \mathbb{Z}^n$, which means $D_1$ must be a principal divisor. □

REFERENCES

[1] I. V. Artamkin. The discrete Torelli theorem. *Mat. Sb.*, 197(8):3–16, 2006.
[2] R. Bacher, P. de la Harpe, and T. Nagnibeda. The lattice of integral flows and the lattice of integral cuts on a finite graph. *Bull. Soc. Math. France*, 125(2):167–198, 1997.
[3] P. Bak, C. Tang, and K. Wiesenfeld. Self-organized criticality. *Phys. Rev. A* (3), 38(1):364–374, 1988.
[4] M. Baker and S. Norine. Harmonic morphisms and hyperelliptic graphs. to appear in *Int. Math. Res. Not.*. Preprint available at arXiv:0701075, 32 pages, 2007.
[5] M. Baker and S. Norine. Riemann-Roch and Abel-Jacobi theory on a finite graph. *Adv. Math.*, 215(2):766–788, 2007.
[6] A. Ben-Israel and T. N. E. Greville. *Generalized inverses*. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, 15. Springer-Verlag, New York, second edition, 2003. Theory and applications.
[7] N. Biggs. *Algebraic graph theory*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, second edition, 1993.
[8] N. Biggs. Algebraic potential theory on graphs. *Bull. London Math. Soc.*, 29(6):641–682, 1997.
[9] N. Biggs. Chip-firing and the critical group of a graph. *J. Algebraic Combin.*, 9(1):25–45, 1999.
[10] N. Biggs. The critical group from a cryptographic perspective. *Bull. Lond. Math. Soc.*, 39(5):829–836, 2007.
[11] S. R. Blackburn. Cryptanalysing the critical group: Efficiently solving Biggs’s discrete logarithm problem, 2008. Cryptology ePrint Archive, Report 2008/170.
[12] B. Bollobás. *Modern graph theory*, volume 184 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998.
[13] S. Bosch and D. Lorenzini. Grothendieck’s pairing on component groups of Jacobians. *Invent. Math.*, 148(2):353–396, 2002.
[14] L. Caporaso and F. Viviani. Torelli theorem for graphs and tropical curves. 2009. Preprint available at arXiv:0901.1389v2.
[15] S. Chen and S. K. Ye. Critical groups for homeomorphism classes of graphs. *Discrete Math.*, 309(1):255–258, 2009.
[16] D. Dhar. Self-organized critical state of sandpile automaton models. *Phys. Rev. Lett.*, 64(14):1613–1616, Apr 1990.
[17] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.
[18] A. H. Durfee. Bilinear and quadratic forms on torsion modules. *Advances in Math.*, 25(2):133–164, 1977.
[19] A. Gabrielov. Abelian avalanches and Tutte polynomials. *Phys. A*, 195(1-2):253–274, 1993.
DLP ON THE JACOBIAN OF FINITE GRAPHS

[20] D. Lorenzini. Arithmetical graphs. Math. Ann., 285(3):481–501, 1989.
[21] D. Lorenzini. Smith normal form and Laplacians. J. Combin. Theory Ser. B, 98(6):1271–1300, 2008.
[22] A. J. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inform. Theory, 39(5):1639–1646, 1993.
[23] G. Mikhalkin and I. Zharkov. Tropical curves, their Jacobians and theta functions. In Curves and abelian varieties, volume 465 of Contemp. Math., pages 203–230. Amer. Math. Soc., Providence, RI, 2008.
[24] G. Musiker. The critical groups of a family of graphs and elliptic curves over finite fields. 2008. to appear in Journal of Algebraic Combinatorics. Preprint available at http://dx.doi.org/10.1007/s10801-008-0162-z.
[25] V. V. Nikulin. Integer symmetric bilinear forms and some of their geometric applications. Izv. Akad. Nauk SSSR Ser. Mat., 43(1):111–177, 238, 1979.
[26] M. Raynaud. Spécialisation du foncteur de Picard. Inst. Hautes Études Sci. Publ. Math., (38):27–76, 1970.
[27] F. Shokrieh. Chip-firing games, g-parking functions, and an efficient bijective proof of the matrix-tree theorem. Submitted, 2009.
[28] J. van den Heuvel. Algorithmic aspects of a chip-firing game. Combin. Probab. Comput., 10(6):505–529, 2001.

GEORGIA INSTITUTE OF TECHNOLOGY, ATLANTA, GEORGIA 30332-0160, USA
E-mail address: shokrieh@math.gatech.edu, farbod@ece.gatech.edu