Final Report for Period: 01/2011 - 06/2011
Submitted on: 12/09/2012
Principal Investigator: Lipton, Richard J.
Award ID: 0902717
Organization: Georgia Tech Research Corp
Submitted By:
Lipton, Richard - Principal Investigator
Title:
SGER: A Proposal For Research Into The Jacobians Of Graphs

Project Participants

Senior Personnel

Name: Lipton, Richard
Worked for more than 160 Hours: Yes
Contribution to Project:

Post-doc

Graduate Student

Name: Shokrieh, farbod
Worked for more than 160 Hours: Yes
Contribution to Project:
Farbod is doing his PhD on this topic. He is an expert now on Jacobians and many of the results are his.

Undergraduate Student

Technician, Programmer

Other Participant

Name: baker, matt
Worked for more than 160 Hours: Yes
Contribution to Project:
Someone that we talk to about the research. He works in the same area.

Research Experience for Undergraduates

Organizational Partners

Other Collaborators or Contacts

I have discussed this work with my other graduate students.

Activities and Findings

Research and Education Activities:
In research the main work has been with Farbod on proving a number of theorems on the Jacobians of graphs.

I have also been writing a theory blog and have highlighted his work there. Probably ~1,000
people have read about work.

Findings: (See PDF version submitted by PI at the end of the report)

Our potential theory methods allow us to prove some new results about chip-firing games and to give new proofs and/or generalizations of some known results in the subject. We also show that certain ``ad-hoc'' techniques in the literature are naturally explained or unified by our approach. In particular, we characterize reduced divisors (G-parking functions) on graphs as the solution to an energy (or potential) minimization problem and we provide an algorithm to efficiently compute reduced divisors. Applications include an ``efficient bijective'' proof of Kirchhoff's matrix-tree theorem and a new algorithm for finding random
spanning trees. The running time of our algorithms are analyzed using potential theory and we show that the bounds thus obtained generalize and improve upon several previous results in the literature. We also study some analogous questions in the context of {\em metric graphs} (or ``abstract tropical curves").

Training and Development:

Farbod is learning how to write and present his work. This is a real challenge, since his work
is really a mix of hardcore math and computer science theory.

Outreach Activities:

The main outreach is via my blog GLL

Journal Publications

Books or Other One-time Publications

MATTHEW BAKER AND FARBOD SHOKRIEH, "CHIP-FIRING GAMES, POTENTIAL THEORY ON GRAPHS, AND SPANNING TREES", (2011). Book, Submitted
Collection: Undecided
Bibliography: none yet

Web/Internet Site

Other Specific Products

Contributions

Contributions within Discipline:

The main results are a better understanding of the Jacobian of a graph. We have the first polynomial algorithms for a variety of questions on the chip firing game.

I would also say the most exciting contribution is the ability to now generate multiple random spanning trees with any distribution. This can be done much more efficiently than ever before. I think this could be an important result.

Contributions to Other Disciplines:

Yes two papers are now available.

Contributions to Human Resource Development:

Contributions to Resources for Research and Education:

Contributions Beyond Science and Engineering:

The main contribution here is through my blog. I reach about 1,000 people per day with this
and related findings.

Conference Proceedings

Categories for which nothing is reported:

Organizational Partners

Any Journal

Any Web/Internet Site

Any Product

Contributions: To Any Human Resource Development

Contributions: To Any Resources for Research and Education

Any Conference

Connections between Potential Theory, Chip-firing Dynamics and Algebraic Geometry*

December 9, 2012

Here is a report from Farbod Shokrieh who worked on most of the research on this project.

My work is primarily concerned with the development of new connections between graph theory, matroid theory, and algebraic geometry. Here is a summary of my current published results. I do have other results and work in progress, which I will be acknowledging the grant support once the work is final. For technical details we refer to the attached papers.

Summary of current results.

(1) The monodromy pairing and discrete logarithm on the Jacobian of finite graphs [2].

Every graph has a canonical finite abelian group attached to it. The construction of this group closely mirrors the construction of the Jacobian variety of an algebraic curve. Motivated by this analogy, it was suggested by Norman Biggs that the critical group of a finite graph is a good candidate for doing discrete logarithm based cryptography. 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.

(2) Chip-firing games, potential theory on graphs, and spanning trees [1].

There is a close connection between chip-firing games and potential theory on graphs. We explore some new aspects of this interplay. Conceptually,

*For final report for NSF grant CCF-0902717 (PI Richard Lipton).

this connection should not come as a surprise; in both settings the Laplacian operator plays a crucial rule. However, in chip-firing games an extra "integrality condition" is imposed; in the language of optimization theory, chip-firing games lead to integer programing problems whose associated linear programming relaxations can be solved using potential theory on graphs.

Our potential theory methods allow us to prove some new results about chip-firing games and to give new proofs and/or generalizations of some known results in the subject. We also show that certain "ad-hoc" techniques in the literature are naturally explained or unified by our approach. In particular, we characterize reduced divisors (G-parking functions) on graphs as the solution to an energy (or potential) minimization problem and we provide an algorithm to efficiently compute reduced divisors. Applications include an "efficient bijective" proof of Kirchhoff's matrix-tree theorem and a new algorithm for finding random spanning trees. The running time of our algorithms are analyzed using potential theory and we show that the bounds thus obtained generalize and improve upon several previous results in the literature. We also study some analogous questions in the context of *metric graphs* (or "abstract tropical curves").

References

[1] M. Baker and F. Shokrieh. Chip-firing games, potential theory on graphs, and spanning trees. Submitted. Preprint available at `arXiv:1107.1313`, 32 pages, 2011.

[2] F. Shokrieh. The monodromy pairing and discrete logarithm on the Jacobian of finite graphs. *J. Math. Cryptol.*, 4(1):43–56, 2010.

Summary of the work on Proposal

Richard J. Lipton

October 2, 2009

The work on this project has been centered around Farbod Shokrieh PhD research. He has worked on two main areas so far.

- **Chip-Firing Games, G-Parking Functions, and the Matrix-Tree Theorem**

  Kirchhoff's matrix-tree theorem states that the number of spanning trees of a graph G is equal to the value of the determinant of the reduced Laplacian of G. We outline an efficient bijective proof of this theorem, by studying a canonical finite abelian group attached to G whose order is equal to the value of same matrix determinant. More specifically, we show how one can efficiently compute a bijection between the group elements and the spanning trees of the graph. The main ingredient for computing the bijection is an efficient algorithm for finding the unique G-parking function (reduced divisor) in a linear equivalence class defined by a chip-firing game. We also give applications, including a new and completely algebraic algorithm for generating random spanning trees. Other applications include algorithms related to chip-firing games and sandpile group law, as well as certain algorithmic problems about the Riemann-Roch theory on graphs.

- **The Monodromy Pairing and Discrete Logarithm on the Jacobian of Finite Graphs**

  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.

The work has been sent to a conference, SODA, without success. We plan on re-writing and resubmitting to another conference.

Also a high level "nugget" of this work so far is the following. There are many algorithms for generating a random spanning trees for a graph. Farbod's main result solves the following problem:

> *Given a graph G, generate k spanning trees for G that has some given joint distribution.*

The previous best methods for doing this were to replace the graph G by its k fold cartesian product, and then apply the standard random walk method. The problem, of course, with method is that the cost is exponential in k. Our new method grows only linearly in k. We think that this application of the Jacobian theory could be quite important.