2012 REU in Mathematics Symposium
MG 104

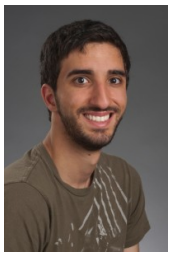
Boise State University
Boise, Idaho

July 26, 2012
10:00 - 1:15

Schedule

9:30 a.m.	Refreshments in the lounge
10:00 - 11:00	*Labeled oriented intervals that are not diagrammatically reducible*
	Presenters: Ashley Earls, Gabriel Islambouli, Rachael Keller and Mingya Yang
11:05 - 11:50	*Ciliate Genome Remodeling*
	Presenters: Chris Anderson, Helen Wauck and Marlena Warner
11:55 - 12:25	*Generalizations of the Advanced Encryption Standard*
	Presenters: Matthew Cole and Kevin Bombardier
12:30 - 1:00	*Elliptic pairs and elliptic reciprocity*
	Presenters: Tom Morrell and Cory Scott
1:05	Closing Remarks.

Labeled Oriented Intervals That Are Not Diagrammatically Reducible

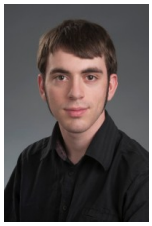
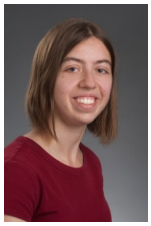
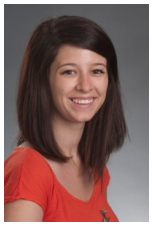



[1]Ashley Earls, [2]Gabriel Islambouli, [3]Rachael Keller, [4]Mingjia Yang, [5]Dr. Jens Harlander (Faculty Mentor)
St Olaf College[1], University of Virginia[2], Louisiana State University[3], Albion College[4], Boise State University[5], Mathematics REU

Presenters: Ashley Earls, Gabriel Islambouli, Rachael Keller and Mingjia Yang.

Knots, which are strings tangled in 3-space, are objects encountered in daily life. The mathematical theory of knots is highly sophisticated, incorporating many classical areas including topology, geometry, combinatorics and group theory. Currently, the study of knots is finding application in fields as diverse as biology, physics and computing. When drawn on a piece of paper, a classical knot is a planar 4-regular graph. A virtual knot, from a graph theoretic point of view, is an arbitrary (not necessarily planar) 4-regular graph. Many questions which have been answered for classical knots are still unanswered for virtual knots. Virtual knots play key roles in long standing conjectures, such as Whitehead's asphericity conjecture. The project is concerned with the topology, geometry and complexity of virtual knots. It is unknown if all virtual knot complements are aspherical. In fact, most seem diagramatically reducible (DR), which means they are aspherical in a strong combinatorial sense. With the aid of computers about 60 billion virtual knots have been checked and very few are not DR. We investigate spherical diagrams for these virtual knots and hope to find general construction principles for non-DR virtual knots.

Ciliate Genome Remodeling

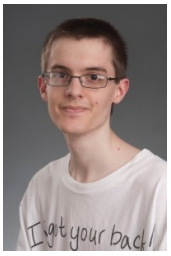
[1]Christopher Anderson, [2]Marlena Warner, [3]Helen Wauck, Dr. [4]Marion Scheepers (Faculty Mentor)
Lewis and Clark College[1], University of Idaho[2], Gustavus Adolphus College[3], Boise State University[4], Mathematics REU

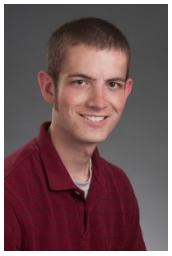
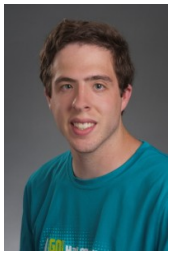
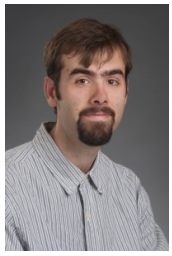
Presenters: Chris Anderson, Helen Wauck and Marlena Warner (INBRE).

Ciliates are single celled organisms hosting two types of nuclei, a micronucleus and a macronucleus. The micronucleus is an encrypted version of the macronucleus. The complexity of the encryption schemas

observed in some species indicate that the ciliate decryptome is capable of executing sophisticated algorithmic tasks. Evidence from ciliate laboratories indicate that the ciliate decryptome is programmable. With the future aim of harnessing the decryptome's capabilities for biomedical, mathematical and technological applications we initiated an investigation into the computational capabilities, efficiency and algorithmic steps of the postulated operations performed by the decryptome. The Department of Cell Biology at the University of Witten-Herdecke (Germany) provided DNA from different stages of decryptome processing of the ciliate Stylonychia lemnae. Using standard laboratory techniques we are tracking the computational steps performed by S.lemnae's decryptome in decrypting micronuclear precursors of the Actin I gene and the alpha-telomere binding protein gene. Some of our laboratory findings suggests a decryptome preference for some computational steps over others. Our mathematical findings include the theorem that a commonly occurring encryption pattern is the unique pattern satisfying certain efficiency and competence criteria. We also found a representation of the ciliate decryption operations as edge modifying operations on certain directed graphs. This representation may enable us to characterize the efficiency of and constraints on the ciliate decryptome. The software we are developing provides computational tools for the analysis of the ciliate decryption process, for rapid experimental planning and for the rapid evaluation of experimental results.

Generalizations of the Advanced Encryption Standard



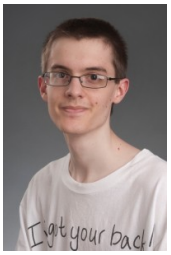
[1]Kevin Bombardier, [2]Matthew Cole, [3]Thomas Morrell, [4]Cory Scott, [5]Dr. Liljana Babinkostova (Faculty Mentor)
Wichita State University[1], University of Notre Dame[2], Washington University in Saint Louis[3], Colorado College[4], Boise State University[5], Mathematics REU

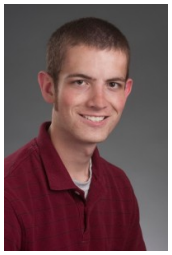
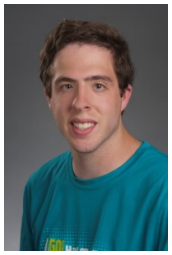
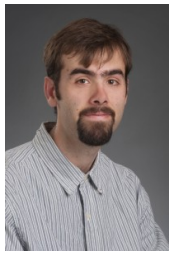
Presenters: Kevin Bombardier and Matthew Cole.

It is well-known that due to a variety of factors, cryptosystems in general become less secure over time. While an aging cryptosystem can simply be replaced, adoption of a completely new standard is often inconvenient. One solution, then, is repeated application of the cryptosystem in question. However, if the encryption functions form a group under functional composition, then no security is gained by repeated encryption.

The Advanced Encryption Standard (AES) is a U.S. Federal Information Processing Standards approved cryptosystem and is used by the U.S. Federal Government for securing top secret information. Since its acceptance in 2001, AES has become widely used also in a variety of commercial and private applications. AES has a highly algebraic structure and could therefore be vulnerable to algebraic attacks. This motivates the investigation of the structural and algebraic aspects of this cryptosystem. We showed that there are algebraic platforms for the AES algorithm over which the encryption functions do not form a group. These results indicate how using a new algebraic platform in the AES algorithm can enhance its security. Even if the encryption functions of AES do not form a group, they generate a group. The structure and the size of the generated group has implications for the security of AES. We showed that depending on the algebraic platform and standards used in the AES algorithm the generated group is either the alternating group or else the symmetric group. We also determined the criteria under which the AES algorithm generates these groups.

Elliptic pairs and Elliptic reciprocity



[1]Kevin Bombardier, [2]Matthew Cole, [3]Thomas Morrell, [4]Cory Scott, [5]Dr. Liljana Babinkostova (Faculty Mentor)
Wichita State University[1], *University of Notre Dame*[2], *Washington University in Saint Louis*[3], *Colorado College*[4], *Boise State University*[5], *Mathematics REU*

Presenters: Thomas Morrell and Cory Scott.

Elliptic Curves are well-known mathematical objects described by Diophantine equations of the form $y^2 = x^3 + ax + b$. Often, such curves are considered over finite fields (i.e. the integers modulo some prime p). An elliptic curve over a finite field will have a finite number of points; if a curve has a prime number of points (including a point at 8), we say it has prime order. Elliptic curves of prime order are particularly well-suited for public-key cryptographic applications, such as Diffie-Hellman Key Exchange, because they are resistant to discrete logarithm attacks such as Silver-Pohlig-Hellman, etc. The public-key cryptosystem based on such elliptic curves is used by the National Security Agency for protecting both classified and unclassified information. We examined the properties of elliptic curves of prime order for the purposes of efficiently generating them, and for creating a "multiplication law" to complement the standard addition law on elliptic curves. This would enable us to construct a field using elliptic curves, allowing them to be utilized in private-key cryptosystems.

We define and examine the notion of an elliptic pair and then use the results to generate elliptic curves of prime order. Furthermore, we investigate problems relating to the distribution of elliptic pairs, such as whether there exist infinitely many elliptic pairs, whether there exist elliptic pairs in particular arbitrary ranges, and how many elliptic pairs exist with prime values less than some given constant.