Fall 2014

- **September 2**
  Organizational Meeting

- **September 9**

  Delaram Kahrobaei (CUNY Graduate Center)
  Conjugacy Problem in Polycyclic Groups and Applications

  Abstract: I will talk about the conjugacy problem in polycyclic groups and some applications. Together with my PhD student Bren Cavallo I recently showed that there are families of polycyclic groups in which the conjugacy problem is NP-complete (IJAC 2014). Polycyclic groups has been proposed for cryptography by Eick and Kahrobaei a couple of years ago, based on computational experiments which conjectured the conjugacy problem for polycyclic groups is in exponential time. Recently together with my former PhD student Ha Lam and Israeli collaborator David Garber, I showed the heuristic algorithm known as Length Based Attack, can not break the cryptosystem using the right parameters (accepted in Journal of Mathematical Cryptology 2014). With Ha Lam we also did some experiments with Heisenberg groups of higher dimensions and noticed that the same result happens (to appear in NPSec'14, Secure Network Protocols, IEEE proceedings, 2014).

- **September 16**

  Joe Brennan (Binghamton University)
  Variation on a Theme of I.D. MacDonald

  Abstract: In a 1963 paper I.D. MacDonald gave an example of a group in which the cyclic commutator subgroup is not generated by a commutator and he gives sufficient conditions on the group G such that its cyclic commutator subgroup is generated by a commutator. The question arises, what is the situation for other words in case the associated word subgroup is cyclic, in particular the word x^n, n a positive integer.

  For n a positive integer, we establish sufficient conditions such that $G^n=\left\langle g^n\,|\, g\in G\right\rangle$ is generated by an n-th power in case G^n is cyclic and give examples of groups G, where G^n is cyclic but not generated by the n-th power of an element. Further, we show that if G^n is cyclic, there exist elements \(g,h \in G\) such that \(G^n = \left\langle g^n, h^n\right\rangle\).

  Joint work with Luise-Charlotte Kappe.

- **September 23**

  Marcin Mazur (Binghamton University)
  Unit producing polynomials

  Abstract: The first part of the talk will be an exposition of some topics about units of group rings. It will lead to some questions about polynomials. The second part will discuss an improvement on a recent result of Broche and del Rio about these questions.

- **September 30**

David Biddle (Binghamton University)
Computing Presentations for the n-Covers of Certain Infinite Classes of Groups

Abstract: The homogeneous n-cover $G(n)$ of a finitely generated group G is a universally characterizable rank n group with quotient G which in essence is the smallest extension of G with 'largest possible' automorphism group (this will be made precise in the talk). The dihedral groups D_k of varying orders $2k$ have covers that have vastly different group structures depending on k (although not 'n'): we will give presentations of various covers of subfamilies of dihedral groups and discuss the growth of both the covers and their massive automorphism groups and if time permits, a discussion of computional limitations imposed on these constructions given by GAP & MAGMA.

- **October 7**

Eran Crockett (Binghamton University)
Supernilpotent quasigroups

Abstract: I will discuss two ways of generalizing the concept of nilpotence to algebraic structures which are not groups. Time permitting, I will mention how one of these generalizations affects the dualizability of a finite algebraic structure.

- **October 14**

Canceled Due To Illness (Rescheduled for Oct. 28)

- **October 21**

Matt Evans (Binghamton University)
Finite Planar Groups

Abstract: A group is called *planar* if the graph of its subgroups is a planar graph. In 2004, Starr and Turner classified all planar Abelian groups. This classification was expanded to all finite groups in 2006 by Bohanon and Reid. In this talk I will state the general classification theorem, but focus my attention on the finite Abelian case by sketching the necessary arguments.

- **October 28**

Jonathan Brown (SUNY Oneonta)
Shifted Twisted Yangians and finite W-algebras

Abstract: Finite W-algebras are certain algebras used to help study the infinite dimensional representation theory of reductive complex Lie algebras. So far they are best understood in type A. This is because, apart from a few isolated cases, there are only presentations of finite W algebras in type A. The key result in finding such presentations, due to Brundan and Kleshchev, is that in type A finite W-algebras are quotients of certain algebras called shifted Yangians, which are subalgebras of the Yangian for gl_n defined in terms of the Yangian's Drinfeld presentation. For the other classical Lie algebras, the role of Yangians is played by twisted Yangians. In this talk I will review some of the representation theory of reductive Lie algebras, as well as the connection between Lie algebra representation theory and finite W-algebra representation theory. Then I will explain how I have defined a Drinfeld presentation for the twisted Yangian associated to so_3, from which I have defined the shifted twisted

Yangian for so_3. This should lead to presentations of a large class of finite W-algebras.

- **November 4**

Nick Devin (Binghamton University)
Wreath products in Thompson's group F

Abstract: Wreath products are extremely abundant among the subgroups of Thompson's group F. I will introduce Matt Brin's notion of a pre-wreath structure, which provides a convenient way recognizing when two elements of F generate a wreath product. We will also see that two certain infinitely iterated wreath products appear as subgroups of F.

- **November 11**

No talk this week

- **November 18**

Joseph Cyr (Binghamton University)
Brain Swapping and Product of Distinct Transpositions

Abstract: In a 2010 episode of the TV show “Futurama” a machine is created which can swap the minds of any two characters who enter. There is one problem however, the same two bodies cannot enter the machine more than once. The question is, after a frenzy of mind-swapping is it possible to undo the switches and put everyone back in their correct bodies? I will be presenting writer Ken Keeler's algorithm for solving this problem, as well as an optimized algorithm from a 2014 paper by Evans, Huang, and Nguyen in The American Mathematical Monthly.

- **November 25**

John Brown (Binghamton University)
A constructive proof of Brauer's Theorem on induced characters in the group ring R(G)

Abstract: We will discuss some of the more interesting parts of a fairly constructive proof of the Brauer Theorem.

- **December 2**

No meeting this week

- **December 9**

Andrew Kelley (Binghamton University)
Profinite groups: Random generation and maximal subgroup growth

Abstract: If we pick a finite subset of a group “at random”, is there a positive probability of generating the whole group? Sometimes, this is in fact the case. After defining profinite groups and giving examples, we will prove* the following theorem of Mann and Shalev: a profinite group G can be generated (topologically) by a random finite subset if and only if G doesn't have too many maximal subgroups. Here, “not too many” means that the maximal subgroup growth (to be defined) is bounded by a polynomial. (*We will need to use one theorem that depends on the classification of finite simple groups, but familiarity with the classification theorem will not be

needed to understand this talk.)