

**LOGIC SEMINAR
SPRING 2006**

Thursday, June 1, 2006

1:00–2:00 p.m.

Speaker: Rumen Dimitrov, Western Illinois University

Place: Old Main (1922 F Street), Room 104

Title: *A structural theorem in modular recursion theory*

Abstract: According to Sacks, it was Friedberg's construction of a maximal recursively enumerable (r.e.) set that sparked interest in the distributive lattice of r.e. sets, modulo finite sets, under inclusion. Among the major results are the Lachlan's characterization of the principal filters of *hh*-simple sets and Soare's proof that the maximal sets form an orbit. We study the modular lattice L^* of r.e. vector spaces, modulo finite dimensional subspaces, under subspace ordering. We are interested in the analogues of the two results mentioned above, as well as in the automorphisms of L^* . In this talk I will present a result characterizing the principal filters of the closures of quasimaximal sets. I will also mention some structural implications concerning automorphisms of the lattice of r.e. sets that generate automorphisms of the lattice L^* .

Thursday, May 11, 2006

4:00–5:00 p.m.

Speaker: Poorvi Vora, Department of Computer Science, GWU

<http://www.seas.gwu.edu/~poorvi>

Place: 1957 E Street, Room 112

Title: *Related-key linear cryptanalysis of block ciphers*

Abstract: We will describe a coding theory framework for related-key linear cryptanalytic attacks on block ciphers. The framework treats linear cryptanalysis as communication, by the adversary, over a low capacity channel, and a related key attack (RKA) as a concatenated code. We will use the framework to show that, in a sense we will make precise, RKAs are asymptotically more efficient than single key attacks.

Note that the above results do not require that the original cipher be vulnerable to related-key attacks, only that it be vulnerable to linear cryptanalysis. This is joint work with Darakhshan Mir. A paper draft describing these results may be found at:

<http://www.seas.gwu.edu/~poorvi/RKA06.pdf>

This talk will be accessible to math and computer science undergraduate students.

General Logic Seminar

Friday, April 28, 2006

4:00–5:00 p.m.

Speaker: Teresa Przytycka, National Center of Biotechnology Information, NLM, NIH

<http://www.ncbi.nlm.nih.gov/CBBresearch/Przytycka/index.html>

Place: 1957 E Street, Room B17

Title: *A new approach to resolving inconsistencies in a set of taxa*

Abstract: Parsimony methods form an important class of methods for construct evolutionary trees. These methods assume that taxa are described by a set of characters

and infer phylogenetic trees by minimizing number of character changes required to explain observed character states. From the perspective of applicability of parsimony methods, it is important to assess whether the characters used to infer phylogeny are likely to provide a correct tree. We introduce a graph theoretical characterization that helps to select correct characters. Given a set of characters and a set of taxa, we construct a network called character overlap graph. We show that the character overlap graph for characters that are appropriate to use in parsimony methods is characterized by significant under-representation of subnetworks known as holes, and provide a mathematical validation for this observation. This characterization explains success in constructing evolutionary trees using parsimony method for some characters (e.g. protein domains) and lack of such success for other characters (e.g. introns). In the latter case, the understanding of mathematical obstacles to applying parsimony methods in a direct way has lead us to a new approach for dealing with inconsistent and/or noisy data. Namely, we introduce the concept of persistent characters, which is similar but less restrictive than the well-known concept of pairwise compatible characters. Application of this approach to introns produces the evolutionary tree consistent with the Coelomata hypothesis. In contrast, the direct application of a parsimony method, using introns as characters, produces a tree which is inconsistent with any of the two competing evolutionary hypotheses. Similarly, replacing persistence with pairwise compatibility does not lead to a correct tree. This indicates that the concept of persistence provides an important addition to the parsimony methods.

Math Colloquium

Friday, April 14, 2006

1:00–2:00 p.m.

Place: 1957 E Street, Room B12

Speaker: John Case, University of Delaware, Department of Computer and Information Sciences

<http://www.cis.udel.edu/~case/>

Title: *Answering the mathematical objection to machine intelligence: An application of machine self-reflection*

Abstract: I briefly consider the standard infinite regress paradox in the notion of a machine “having” a complete model of itself and show how to circumvent it. Then I pictorially present a simple theoretical application of machine self-reflection and use this application as a vehicle to illustrate what Turing in his seminal paper on machine intelligence called the *mathematical objection to machine intelligence*. Lastly I employ machine self-reflection to completely answer this objection, and, in the process, point out a seeming limitation of *human* intelligence that suitably clever machines do not have.

This talk is for undergraduate students, graduate students, and faculty.

Thursday, April 6, 2006

5:15 p.m.–6:00 p.m.

Old Main (1922 F Street), Room 104

Speaker: Valentina Harizanov, GWU

<http://home.gwu.edu/~harizanv/>

Title: *Strong computability theoretic degree spectra*

Abstract: For a computability theoretic reducibility r , the r -degree spectrum of a relation R on a computable structure A is the set of all r -degrees of the images of R in all isomorphic computable copies of A . We focus on degree spectra under truth-table equivalence and weak truth-table equivalence for initial segments of computable linear orderings. We will present some of our very recent results.

Tuesday, April 4, 2006

11:00 a.m.–12:00 noon

Old Main (1922 F Street), Room 104

Speaker: Sarah Pingrey, GWU

<http://home.gwu.edu/~spingrey>

Title: *Interval Trees*

Abstract: Let L be a linear ordering with a least element. An interval tree is a partial function from a leftward-closed, finitely branching tree T whose nodes are sequences of natural numbers with no terminal nodes, to the set of nonempty intervals of L with some special properties. The talk will cover an introduction to interval trees and then discuss the relationships between interval trees and scattered linear orderings and linear orderings of type: natural numbers followed by a copy of integers.

Tuesday, March 28, 2006

11:00a.m.–12:00 noon

Old Main (1922 F Street), Room 104

Speaker: Johanna Franklin, University of California, Berkeley

Title: *Triviality and lowness for effective randomness*

Abstract: When studying effective randomness, it is natural to consider not only random sequences but also sequences that are “far from random.” There are several ways to formalize this concept, including triviality and lowness. Each of these ways can be defined for various randomness notions, such as Martin-Löf, Schnorr, and computable randomness. This talk will give an introduction to these concepts and provide an overview of current work on triviality and lowness. All math, statistics, and computer science graduate students are welcome.

Logic & Topology

Tuesday, March 21, 2006

11:00a.m.–12:00 noon

Old Main (1922 F Street), Room 104

Speaker: Jennifer Chubb, GWU

Title: *Spaces of orderings of semi-groups*

Abstract: A left ordering of a semi-group is a linear ordering of the underlying set that is preserved by multiplication on the left. A right ordering is defined similarly, and a bi-ordering is an ordering that is both a left and right ordering. A natural topology can be defined on the space of orderings of a semi-group, and for certain groups this space is homeomorphic to the Cantor space. Further, when the underlying group is \mathbb{Z}^2 , every Turing degree is realized by an ordering in this space, that is, there are orderings of

arbitrary complexity in the computability theoretic sense. We will discuss these results, see some examples, and consider some related open questions.

Wednesday, March 8, 2006

2:30–3:30 p.m.

Old Main (1922 F Street), Room 104

Speaker: Valentina Harizanov, GWU

<http://home.gwu.edu/~harizanov/>

Title: *Spaces of orders on computable groups*

Abstract: The space of (left) orders of a group G consists of the set of positive cones of all (left) orders on G . We study topological and computability theoretic properties of spaces of orders and left orders on certain computable groups. This is joint work with Dabkowska, Dabkowski and Togha.

Tuesday, March 7, 2006

5:15–6:00 p.m.

Old Main (1922 F Street), Room 104

Speaker: Jennifer Chubb, GWU

Title: *Recovering structures from semigroups of partial automorphisms*

Abstract: We consider the semigroup of all finite partial automorphisms, and the semigroup of all partial computable automorphisms of a countable structure. We show that in some cases, the elementary equivalence of the semigroups of the finite partial automorphisms yields elementary equivalence of the structures themselves, and sometimes isomorphism of the structures. For certain Boolean algebras, we establish that the elementary equivalence of the semigroups of the partial computable automorphisms suffices to provide for the existence of a computable isomorphism of the Boolean algebras. This is joint work with Harizanov, Morozov, Pingrey and Ufferman.

Friday, February 24, 2006

4:00–5:00 p.m.

Old Main (1922 F Street), Room 104

Speaker: Joseph S. Miller, University of Connecticut

<http://www.math.uconn.edu/~josephmiller/>

Title: *The initial segment complexity of random reals*

Abstract: Prefix-free Kolmogorov complexity is one of the fundamental approaches to effective randomness. It allows us to capture the intuition that random reals are incompressible and is an important tool in their study. This talk will give an introduction to Kolmogorov complexity, to Martin-Löf randomness, and to the prefix-free complexity of initial segments of random reals. Recent work allows us to say a great deal about the behaviour of initial segment complexity, but basic open questions remain. All math, statistics, and computer science graduate students are welcome.

Math Logic PhD Specialty Exam Lecture

Thursday, February 23

2:30–4:30 p.m.

1957 E Street, Room B16

Speaker : Sarah Pingrey, Mathematics, GWU

<http://home.gwu.edu/~spingrey>

Title: *Orderings on computable torsion free abelian groups*

Abstract: In 1979, Metakides and Nerode showed that facts about Π_1^0 classes can be transferred directly to the space of orders on computable fields. Solomon looked at the same problem for orderable groups. If G is a computable torsion free abelian group, we will find the complexity of the space of orders on G , depending on the rank of G . Then, we will be able to show Solomon's result that one of the theorems of Metakides and Nerode does not hold, not even in a weak sense.

Logic&Topology

Tuesday, February 21, 2006

11:00 a.m.–12:00 noon

Old Main (1922 F Street), Room 104

Speaker : Zbigniew Oziewicz, Universidad Nacional Autónoma de México

Title: *Braided logic*

Abstract: Joyce, 1979, 1982, and independently Matveev, 1982, introduced a *quandle*, a self-distributive Boolean binary operation that need not be associative. Kauffman, 1991, generalized a quandle to a *crystal*. A related concept, a *rack*, was introduced by Fen and Rourke, 1992; Grana, 2000; Yetter, 2002. Quandle, crystal, and rack are models of the Artin braid axiom and are related to the Reidemeister moves. Drinfeld' in 1992 raised the question of finding models/solutions of the Artin braid axiom in a category of sets, set-theoretic models.

Starting in 1999, jointly with Ernestina Chavez Rodriguez and with Angell Lopez, we became interested in bi-quandles and bi-racks, as the general set-theoretic solutions of the Artin (Yang-Baxter) braid equations. Bi-racks lead to the concept of the braided logic, an algebraic logic whose axiomatization is interesting compared to Boolean algebra. Short review of results will be presented and compared with other approaches (for example, with Lu, Yan, Zhu, 2000).

Wednesday, February 15, 2006

2:30–3:30 p.m.

Old Main (1922 F Street), Room 104

Speaker : Russell Miller, Queens College, CUNY

Title: *The low_n Turing degrees and spectra of structures*

Abstract: Slaman, Wehner, and Hirschfeldt have all constructed structures which distinguish the computable Turing degree $\mathbf{0}$ from the noncomputable degrees, in the sense that the spectrum of each structure consists precisely of the noncomputable degrees. We show that within the Δ_2^0 degrees, the same can be done for a linear order. This is accomplished using the technique of permitting below a Δ_2^0 set, and we include an explanation of the mechanics and intuition behind this type of permitting. We also discuss the liftings of these results by Knight et al. (for the Slaman-Wehner-Hirschfeldt structures) and by Frolov (for the linear order) to build structures whose spectra contain precisely the non- low_n degrees.

Friday, February 3, 2006

2:30–3:30 p.m.

Old Main (1922 F Street), Room 104

Speaker: John Chisholm, Western Illinois University

Title: *Structural properties of computably stable models*

Abstract: A computable model M is *computably stable* provided that, whenever f is an isomorphism between M and another computable model N , then f is computable. The earliest examples of computably stable models had strong computable/structural regularities; but it had been known that the computable regularities were not necessary. We will show that the structural properties also are unnecessary, developing an example of a computably stable model that is not atomic over any finite tuple of points.

Friday, January 27, 2006

2:30–3:30 p.m.

Old Main (1922 F Street), Room 104

Speaker: Valentina Harizanov, GWU

<http://home.gwu.edu/~harizanv/>

Title: *Orders on groups*

Abstract: For a group, a left order is a linear order on its domain, which is left-invariant with respect to the group-theoretic operation. We similarly define a right order and a (bi)order on a group. Every left-orderable group is torsion-free. While every abelian torsion-free group is orderable, not every torsion-free group is even left-orderable. For familiar computable orderable groups, we investigate computability-theoretic properties of their orders.