74th Workshop on General Algebra
74. Arbeitstagung Allgemeine Algebra (AAA74)

Tampere University of Technology
Tampere, Finland

June 7–10, 2007

Contents

A notion of functional completeness for first order structures

Mac Henry Akeh
University of Buea
livinusfusi@yahoo.fr
Coauthors: Marcel Tonga, Temgoua Alomo Etienne Romuald

In this work, we propose a notion of functional completeness for first order structures, and find conditions for a functionally complete structure to have a compatible Pixley function which is term representable on classes.

Multiplication von Neumann regular modules

Majid M. Ali
Department of Mathematics, College of Science, Sultan Qaboos University, Oman
mali@squ.edu.om

A commutative ring with identity R is said to be von Neumann regular if and only if for each element a in R there exists an element x in R such that $a = axa$. It is well known that R is von Neumann if and only if every principal ideal of R is pure if and only if the set of nilpotents of R, $\mathrm{Nil}(R) = 0$ and $\dim(R) = 0$, that is every prime ideal maximal. In this talk, we introduce and investigate the concept of von Neumann regular modules as a natural generalization of von Neumann regular rings. We define the concepts of idempotent and nilpotent submodules of a module as follows: A submodule N of M is idempotent if $N = [N : M]N$ and N is nilpotent if $N = N[N : M] * *k$ for some positive integer k. We say that an element m in M is nilpotent if Rm is nilpotent in M. We show that the following statements are true.

(1) If M is a faithful multiplication module then M is von Neumann regular if and only if R is von Neumann.

(2) If $\mathrm{Nil}(M)$ is the set of nilpotent of M, then $\mathrm{Nil}(M) = \mathrm{Nil}(R)M =$ the intersection of all prime submodules of M.

(3) If M is multiplication module then, M is von Neumann regular if and only if $\mathrm{Nil}(M) = 0$ and $\dim(M) = 0$, that is every prime submodule of M is maximal.

(4) M is a multiplication von Neumann regular module if and only if it is locally simple.

We also investigate the relationship between the concept of von Neumann regular modules and each of prime and Jacobson radicals which we think that it will play an important role in multiplicative theory of modules and ideals.

Decision problems for pseudovarieties

Jorge Almeida
University of Porto, Portugal
jalmeida@fc.up.pt

By a pseudovariety we mean a class of finite algebras that is closed under taking homomorphic images, subalgebras, and finite direct products. In case the algebras are semigroups or monoids, the Eilenberg Correspondence Theorem provides both a strong motivation and a rich source of problems. The theorem translates a large class of combinatorial problems concerning finite automata and the formal languages they recognize to questions which usually amount to decide whether a given finite semigroup belongs to a pseudovariety which is defined by some generating set. The purpose of this talk is to survey this as well as several related decision problems for pseudovarieties.

Semihereditary Bezout rings and semigroups

P. N. Ánh
Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, pf.127, H-1364 Budapest
anh@renyi.hu
Coauthors: M. Siddoway

Divisibility semigroups (i.e., one of principal ideals partially ordered by reverse inclusion) of semihereditary rings can be characterized as semihereditary B-semigroups. The construction is based on a geometry of such semigroups and extends unusually Stone description of Boolean algebras.

Prime submodules and radical formula

Abdulrasool Azizi
Shiraz University
aazizi@shirazu.ac.ir

Let N be a proper submodule of an R-module M. It is said that N is a prime submodule of M, if the condition $ra \in N$, $r \in R$ and $a \in M$ implies that $a \in N$ or $rM \subseteq N$. For every submodule B of M, we consider two versions of radical for B related to prime submodules of M containing B and we compare these two versions.

Clones from ideals, part II

Mathias Beiglböck
TU Vienna
mathias.beiglboeck@tuwien.ac.at
Coauthors: Martin Goldstern, Lutz Heindorf, Michael Pinsker

On an infinite base set X, every ideal of subsets of X can be associated with the clone of those operations on X which map ideal sets to ideal sets. We investigate the position of clones that arise in this way in the clone lattice. In particular we present the solution to two problems of Czédli and Heindorf and establish the existence of $2^{\mathfrak{c}}$ precomplete clones in the clone lattice over a countable set, for the first time without using the Axiom of Choice.

The talk will not start with a quiz on part I (by M. Pinsker).

Extremely noncommutative elements in rings

Howard E. Bell
Brock University
hbell@brocku.ca

An element x of a ring R is called extremely noncommutative if its centralizer is as small as possible—i.e., is equal to the subring $\langle x \rangle$ generated by x. We give a complete characterization of rings in which all nonzero elements are extremely noncommutative, and we discuss rings in which all noncentral elements are extremely noncommutative.

Rough set systems as semiboolean algebras with inversion

Jānis Cīrulis
Department of Computer Science, University of Latvia
jc@lanet.lv

Several descriptions of rough set systems as ordered algebras have been discovered and discussed in the literature. There are close connections between rough set algebras and approximation algebras, double Stone algebras, semisimple Nelson algebras, three-valued Lukasiewicz algebras, bounded BCK-algebras, as well as some other abstract classes of algebras.

We propose a new kind of rough set algebras: semiboolean algebras with inversion. The underlying order structure of these algebras is the so called knowledge ordering:

$$(L,U) \leq (L',U') \quad \text{iff} \quad L \subset L' \text{ and } U' \subset U$$

rather than the more usual inclusion ordering:

$$(L,U) \subset (L',U') \quad \text{iff} \quad L \subset L' \text{ and } U \subset U'.$$

The main result presented in the paper is a representation theorem of semi-boolean algebras with inversion.

How does variable identification affect the essential arity of finite functions?

Miguel Couceiro
Dep. Mathematics, Statistics and Philosophy, University of Tampere
miguel.couceiro@uta.fi
Coauthors: Erkko Lehtonen

By a finite function we simply mean a map $f\colon A^n \to B$ where n is a positive integer called the arity of f, A is a nonempty finite set and B is a possibly different nonempty set, not necessarily finite. Typical examples are the Boolean functions when $A = B = \{0, 1\}$ and the pseudo-Boolean functions when $A = \{0, 1\}$ and B is the set of real numbers.

The essential arity of a finite function $f\colon A^n \to B$ is defined as the number of essential variables of f, that is, variables x_i such that there are $a_1, \ldots, a_{i-1}$, a_i, b_i, $a_{i+1}, \ldots, a_n \in A$ such that

$$f(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, b_i, a_{i+1}, \ldots, a_n).$$

In this presentation we shall discuss the effect that the operation of identification of variables has on the essential arity of finite functions. We survey some recent results of current research on the theory of essential variables being developed jointly with Erkko Lehtonen (Tampere University of Technology).

Homogeneity in congruence modular varieties

Dejan Delic
Ryerson University, Toronto, Canada
ddelic@ryerson.ca

The concept of homogeneity of a struture is one of fundamental notions in model theory. Namely, we say that a (countable) structure is homogeneous if every isomorphism between two of its (finite) substructures can be extended to an automorphism of the original structure. In other words, the structure of the automorphism group is completely determined by the orbits of the action on finite substructures.

In this talk, we will try to present some results related to variations of homogeneity in finitely generated congruence modular varieties and investigate what repercussions these results bear to the problem of the classification of the locally finite varieties with the decidable first-order theory.

Semigroups of n-ary operations

Klaus Denecke
University of Potsdam, 14469 Potsdam, Am Neuen Palais 10
kdenecke@rz.uni-potsdam.de
Coauthors: Runglawan Butkote

An abstract clone is a multi-based algebra

$$\mathcal{C} := ((C^{(n)})_{n\geq 1}, (S^n_m)_{m,n\geq 1}, (e^n_i)_{1\leq i\leq n}), \quad (m,\, n \text{ integers})$$

with $n+1$-ary operations S^n_m and nullary operations e^n_i, which is an element of a variety of multi-based algebras defined by the so-called superassociative law and two more identities.

Let $a, b \in C^{(n)}$. Then $a + b := S^n_n(a, b, \ldots, b)$ defines a binary associative operation $+$ on $C^{(n)}$ and one obtains a semigroup $(C^{(n)}; +)$. We study a concrete version of this semigroup, the semigroup of all n-ary operations defined on a finite non-empty set A.

Let $O^n(A)$ be the set of all n-ary operations defined on the finite set A. If $|A| = k \geq 2$, the elements of $O^n(A)$ are called n-ary functions of k-valued logic. If $f \in O^n(A)$ and $g_1, \ldots, g_n \in O^m(A)$, we define the superposition operation $S^{n,A}_m$ by $S^{n,A}_m(f, g_1, \ldots, g_n)(a_1, \ldots, a_m) := f(g_1(a_1, \ldots, a_m), \ldots, g_n(a_1, \ldots, a_m))$ for all $a_1, \ldots, a_m \in A$. Together with the projections $e^{n,A}_i : A^n \to A, i \leq n$, defined by $e^{n,A}_i(a_1, \ldots, a_n) := a_i$ for all $a_1, \ldots, a_n \in A$ we get the multi-based algebra

$$((O^n(A))_{n\geq 1}, (S^{n,A}_m)_{m,n\geq 1}, (e^{n,A}_i)_{1\leq i\leq n})$$

which is a model of the clone axioms. Alternatively, instead of clones of operations, we may study the properties of the semigroup $(O^n(A); +)$ and its subsemigroups and are especially interested in the following problems:

1. Determine the order of all elements of $(O^n(A); +)$.
2. Determine all regular elements of $((O^n(A); +)$.
3. Characterize all subsemigroups of $(O^n(A); +)$ satisfying certain identities.
4. Characterize Green's relations.

Some congruence properties in single algebras

Gerhard Dorfer
Vienna University of Technology, Institute of Discrete Mathematics and Geometry
g.dorfer@tuwien.ac.at
Coauthors: Ivan Chajda, Helmuth Länger

Some local versions of congruence permutability, regularity, uniformity and modularity are investigated. The results are applied to several examples including implication algebras and orthomodular lattices.

Collapsing monoids consisting of permutations and constants

Miklós Dormán
University of Szeged, Hungary
dorman@math.u-szeged.hu

We determine all collapsing transformation monoids that contain at least one unary constant operation and whose nonconstant operations are permutations. Furthermore, we describe a subclass of transformation monoids that consist of at least three unary constant operations and some permutations for which the corresponding monoidal intervals are 2-element chains.

On a cryptographical characterization of classical and nonclassical event systems

Dietmar Dorninger
Vienna University of Technology
D.Dorninger@tuwien.ac.at
Coauthors: E. Beltrametti and M. Maczynski

Systems of numerical events as well as a more general notion of fields of events, which arise from a generalization of the one-to-one correspondence between Boolean algebras and Boolean rings to a correspondence between lattices with an antitone involution and ring-like quantum logics known as generalized Boolean quasirings, are studied under a common viewpoint.

This common viewpoint is to relate events to an equation which is characteristic for fully symmetric cryptographic systems, namely $(x + s) + s = x$ for all plain text messages x, which are encrypted and deciphered by means of a secret key s and an operation $+$. The encryption function $K_s(x) := x + s$ is an involution, and we will show that one can link this involution to the separation between the classical and the quantum behaviour.

In the first place a class of generalized Boolean quasirings is investigated which leads to a notion of event fields that appears appropriate also in the quantum framework. Then the classical case is characterized by means of the above mentioned property of fully symmetric ciphers. An analogous result for systems of numerical events that can be partially ordered but are not lattices in general is derived and related to the previous findings. Finally a possible physical interpretation of the presented results will be given.

Semilattices with sectional mappings

Günther Eigenthaler
Vienna University of Technology, Institute of Discrete Mathematics and Geometry
g.eigenthaler@tuwien.ac.at
Coauthors: Ivan Chajda

We consider join-semilattices S with 1 where for every element p of S a mapping on the interval $[p, 1]$ is defined; these mappings are called sectional mappings and such structures are called semilattices with sectional mappings. We assign to every semilattice with sectional mappings a binary operation which enables us to classify the cases where the sectional mappings are involutions and/or antitone mappings. There are connections to some earlier results (2004, 2005) of Ivan Chajda (and coauthors), and also to a paper of J.C. Abbott (1967) on "Semi-Boolean algebras".

Groupoids with quasigroup and Latin square identities

Jan Gałuszka
Institute of Mathematics, Silesian University of Technology
jan.galuszka@polsl.pl

Connections of some groupoid identities with the quasigroup and Latin square properties are investigated using combinatorial methods.

Characterizing distributive lattices by their double skeletons

Joanna Grygiel
Jan Dlugosz University, Częstochowa, Poland
j.grygiel@ajd.czest.pl

We introduce a notion of a weighted double skeleton of finite distributive lattices, which provides some characterization of the lattices. We show that many important properties of finite distributive lattices can be read from their weighted double skeleton, which means that in the situation when we deal with very big lattices (e.g., in data structures or in Dedekind's problem) it may be convenient to consider the weighted double skeleton instead of the lattice itself.

Coalgebraic modal logic

H. Peter Gumm
Philipps-Universität Marburg
`gumm@mathematik.uni-marburg.de`

The famous result of Hennessy and Milner for modal logic on Kripke structures can, after work of Pattinson and Schröder, be faithfully carried over to arbitrary coalgebras whose type functor is separable.

We give a simplified and more elegant account of their logic and present some concrete examples. Finally, we provide a characterization of separable functors.

Term definable classes of Boolean functions and frame definability in modal logic

Lauri Hella
Department of Mathematics, Statistics and Philosophy, University of Tampere
`lauri.hella@uta.fi`
Coauthors: Miguel Couceiro and Jari Kivelä

We establish a connection between term definability of Boolean functions and definability of finite modal frames. We introduce a bijective translation between functional terms and uniform degree-1 formulas and show that a class of Boolean functions is defined by a set of functional terms if and only if the corresponding class of Scott-Montague frames is defined by the translations of these functional terms, and vice versa.

As a special case, we show that the clone Λ_1 of all conjunctions corresponds to the class of all Kripke frames. We also characterize some classes of Scott-Montague frames that correspond to subclones of Λ_1 by restricting the class of Kripke frames in a natural way. Furthermore, by modifying Kripke semantics, we extend our results to correspondences between the linear clones and classes of Kripke frames equipped with modified Kripke semantics.

The complexity of identity checking over finite groups

Gábor Horváth
University of Hertfordshire, Hatfield, United Kingdom
`G.Horvath@herts.ac.uk`
Coauthors: Csaba Szabó (Eötvös Loránd University, Budapest, Hungary)

The talk is about determining the complexity of checking an identity over a given finite algebra. This question has been answered completely for finite rings and dichotomy has been proved. For finite groups the answers are far from complete. I will give a brief summary of the results about the complexity of checking an identity over a given finite group. I will show the methods by which these results can be proved.

Convexities of partial monounary algebras

Danica Jakubíková-Studenovská
Faculty of Science, P.J. Šafárik University, Košice, Slovakia
danica.studenovska@upjs.sk

E. Fried defined a convexity of lattices as a nonempty class of lattices closed under homomorphisms (H), direct products (P) and convex sublattices (C). Convexities of partial monounary algebras are defined analogously. Later it was proved that the system of all convexities of lattices forms a proper class. We present results concerning convexities of partial monounary algebras. We can show that the convexity generated by a class T of partial monounary algebras is equal to HCP(T). On the contrary to the power of the system of all convexities of lattices, the system of all convexities of partial monounary algebras is finite: it consists of 23 elements. There are 13 principal convexities. In particular, the convexity containing all partial monounary algebras is principal, too.

Pawlak's information systems in terms of Galois connections and functional dependencies

Jouni Järvinen
Turku Centre for Computer Science (TUCS), 20014 University of Turku, Finland
jjarvine@utu.fi

Armstrong axioms determine a closed set of formal implications—called functional dependencies—that hold in a database relation. Dependency relations can be also found in, for example, formal concept analysis, dependence spaces, and Pawlak's information systems. Alan Day studied functional dependencies in a more general setting of complete lattices and defined Armstrong systems as sets of ordered pairs satisfying certain conditions analogous to Armstrong's original axioms. In this talk we point out that Galois connections and Armstrong systems are closely connected—we show that every Galois connection between two complete lattices determines an Armstrong system.

The model for attribute-based information systems considered here was introduced in 1970s by Zdzislaw Pawlak. He also gave the notions and fundamental properties of indiscernibility relations, dependencies between attribute sets, attribute reduction, and information languages. We show that in information systems Galois connections are found between all subsets of attributes and binary relations on the object set of Pawlak's information systems. Then information systems are described in terms of the corresponding Armstrong systems. In particular, it is shown that the entries of the indiscernibility matrix of an information system form a dense set and the reducts are characterized in terms of dense sets.

A semi-generalization of the Loop lemma for chain-complete orthoalgebras

Gejza Jenča
Slovak University of Technology in Bratislava
gejza.jenca@stuba.sk

In 1971, R. Greechie proved that a certain type of quantum logics (nowadays known as *Greechie logics*) is an orthomodular lattice if and only if the logic in question does not contain a loop of length 3 or 4. This result (called *Loop lemma*) is widely used by the quantum logicians to construct complicated examples of finite orthomodular lattices.

We present a generalization of one of the implications of the Loop lemma: if a chain-complete orthoalgebra is not lattice ordered, then the semilattice of sets generated (in a certain way) by the blocks must contain at least one subposet that is isomorphic to a 2, 3 or 4-crown.

Testing polynomiality for finite expanded groups: survey and perspectives

Kalle Kaarli
University of Tartu
kaarli@math.ut.ee

Expanded group is a universal algebra having a group reduct. Let A be a finite algebra. We say that a function $f : A^k \to A$ has an n-interpolation property if for every subset $X \subseteq A^k$ of size n there is a k-ary polynomial function p of A such that the restrictions of f and p to X coincide. Clearly, f has the n-interpolation property iff it preserves all diagonal subuniverses of A^n. Also, f is a polynomial of A iff it has the n-interpolation property where $n = |A|^k$. It happens rather often that, given a finite expanded group A, a function defined on A is a polynomial provided it satisfies the n-interpolation property where n is a relatively small fixed integer. That is, the polynomiality can be tested by subuniverses of A^n where n is relatively small. We give a survey of results of this type and list open problems.

Rings with feedback cyclization property

Hermann Kautschitsch
University of Klagenfurt, Austria
hermann.kautschitsch@uni-klu.ac.at

The Feedback Cyclization Property (FC-property) is a stronger form of the Pole Assignability Property. The dynamic behaviour of linear systems over those rings can be improved by a feedback matrix such that the new system matrix has desired eigenvalues. In case of FC-property one can reduce the system to a single input. It is shown how many known results can be unified by considering special homomorphisms. Considering linear systems with time delays leads to matrices over polynomial rings. It is not known whether the polynomials over the complex numbers have the FC-property or not. A new necessary condition is given and results over special polynomial rings are derived.

New characterization of Boolean algebras by Elkan's formula

Michiro Kondo
Tokyo Denki University
kondo@sie.dendai.ac.jp

In this talk, we give a new characterization of Boolean algebras in terms of a special equation called here Elkan's formula (E) $(x \wedge y')' = y \vee (x' \wedge y')$. It means that, for any bounded lattice $L = (L, \wedge, \vee, ', 0, 1)$ with a unary operator $'$, if it satisfies the following conditions (c1) $1' = 0$ and (E) then it is a Boolean algebra. Moreover we consider mathematical properties of bounded lattices satisfying Elkan's formula (E).

On I-A-groups

Gerhard Kowol
Faculty of Mathematics, University of Vienna, Austria
gerhard.kowol@univie.ac.at

Let G be a finite group and let $I(G)$ resp. $A(G)$ be the nearrings generated by the inner resp. all automorphisms of G with respect to the extended group operation and composition. Groups for which $I(G) = A(G)$ holds are called I-A-groups. Only few examples are known mostly if the lattice of normal subgroups is small. Applying the concept of polynomial functions on groups we show among others that nilpotent I-A-groups necessarily have to be directly indecomposable and solve the case of class 2 completely.

Generators in the category of S-posets

Valdis Laan
University of Tartu
vlaan@ut.ee

We give some characterizations of generators and cyclic projective generators in the category of ordered right acts over an ordered monoid.

Equivalence of operations with respect to discriminator clones

Erkko Lehtonen
Tampere University of Technology
erkko.lehtonen@tut.fi
Coauthors: Ágnes Szendrei (University of Colorado, Boulder and Bolyai Institute, Szeged)

For each clone $\mathcal{C}$ on a set A there is an associated equivalence relation, called $\mathcal{C}$-equivalence, on the set of all operations on A, which relates two operations iff each one is a substitution instance of the other using operations from $\mathcal{C}$. We prove that if $\mathcal{C}$ is a discriminator clone on a finite set, then there are only a finite number of $\mathcal{C}$-equivalence classes. Moreover, we show that the smallest discriminator clone is minimal with respect to this finiteness property. For discriminator clones of Boolean functions we explicitly describe the associated equivalence relations.

Polynomial functions on the units of $\mathbb{Z}_{2^n}$

Smile Markovski
Ss Cyril and Methodius University, Faculty of Sciences, Institute of Informatics, p.f. 162, Skopje, Macedonia, email: smile@ii.edu.mk
smile@ii.edu.mk
Coauthors: Danilo Gligoroski, Centre for Quantifiable Quality of Service in Communication Systems, Norwegian University of Science and Technology, O.S. Bragstads plass 2E, N-7491 Trondheim, Norway, email: gligoroski@yahoo.com & Zoran Šunić, Department of Mathematics, Texas A&M University, College Station, TX 77843-3368, USA, email: sunic@math.tamu.edu

Polynomial functions on the group of units Q_n of the ring $\mathbb{Z}_{2^n}$ are considered. A finite set of reduced polynomials $\mathbb{RP}_n$ in $\mathbb{Z}_{2^n}[x]$, that induces the polynomial functions on Q_n is determined. Each polynomial function on Q_n is induced by a unique reduced polynomial, the reduction being made using a suitable ideal in $\mathbb{Z}_{2^n}[x]$. The set of reduced polynomials forms a multiplicative 2-group. The results obtained are used to efficiently construct families of exponential cardinality of, so called, huge quasigroups and huge k-ary quasigroups of order 2^{n-1}, which are useful in the design of various types of cryptographic primitives.

A ternary operation structure motivated by cryptographical functions

Gerasimos Meletiou
TEI of Epirus, P.O. Box 110, Arta 47100, Greece
gmelet@teiep.gr
Coauthors: Tasos Patronis

If a is a generator of the multiplicative group F^* of a finite field F, the Diffie–Hellman mapping from $F^* \times F^*$ to F^* is defined by

$$(x, y) \mapsto a^{\log_a(x) \log_a(y)}$$

where $\log_a$ is the well-known Discrete Logarithm function.

If a runs over all generators of F^* and x, y run over F^*, then the ternary operation $[xay] := a^{\log_a(x) \log_a(y)}$ has a number of interesting properties. This algebraic structure can be represented by means of Vandermonde matrices over the field F.

On matrix partial orderings

Jorma K. Merikoski
Department of Mathematics, Statistics and Philosophy, FI-33014 University of Tampere, Finland
jorma.merikoski@uta.fi

Let $\mathbf{R}^{n\times n}$ and $\mathbf{C}^{n\times n}$ be the spaces of real and respectively complex n-by-n matrices. We study the following partial orderings ("p.o." in the sequel) on these spaces.

If $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij}) \in \mathbf{R}^{n\times n}$, define

$$\mathbf{A} \leq^{el} \mathbf{B} \quad \Leftrightarrow \quad a_{ij} \leq b_{ij} \text{ for all } i,\ j \quad \text{(elementwise p.o.).}$$

On $\mathbf{C}^{n\times n}$, define

$$\begin{aligned} \mathbf{A} \leq^{L} \mathbf{B} &\quad \Leftrightarrow \quad \mathbf{B} - \mathbf{A} \text{ is Hermitian and nonnegative definite} \\ \mathbf{A} \leq^{*} \mathbf{B} &\quad \Leftrightarrow \quad \mathbf{A}^*\mathbf{A} = \mathbf{A}^*\mathbf{B} \text{ and } \mathbf{A}\mathbf{A}^* = \mathbf{B}\mathbf{A}^* \\ \mathbf{A} \leq^{rs} \mathbf{B} &\quad \Leftrightarrow \quad \operatorname{rank}(\mathbf{B} - \mathbf{A}) = \operatorname{rank}\mathbf{B} - \operatorname{rank}\mathbf{A} \end{aligned}$$

(Löwner p.o., star p.o., rank subtractivity p.o., respectively). Here $\mathbf{A}^*$ denotes the conjugate transpose of $\mathbf{A}$.

The ring of graph invariants

Tomi Mikkonen
Tampere University of Technology
`tomi.mikkonen@tut.fi`

All graph invariants can be represented as linear combinations of what we call basic graph invariants. We denote the basic graph invariants by $I(g)(h)$ and they calculate the number of subgraphs of h isomorphic to g. Basic invariants are algebraically dependent. The structure of this ring is discussed, as well as the algebraic dependencies which the basic invariants satisfy. We derive lower and upper bounds for the minimal number of basic graph invariants needed for graph isomorphism.

Unlabeled graphs are in 1–1 correspondence with the graph invariants $I(g)$ that they specify. It turns out that certain structured sets of graphs/graph invariants and their internal properties imply inequalities which are useful in solving e.g. Ramsey numbers and other extremal problems in graph theory.

Higher commutators in Mal'cev algebras: properties and applications

Nebojša Mudrinski
Department of Algebra, JKU Linz, Austria
`mudrinski@algebra.uni-linz.ac.at`
Coauthors: Erhard Aichinger, Department of Algebra, JKU Linz, Austria

We are interested in the following problem:

> Given a finite Mal'cev algebra $\mathbf{A}$, can the clone of polynomial functions be described by finitely many relations on R?

More precisely, for a given finite Mal'cev algebra $\mathbf{A}$, we ask the following: Is there a *finite* set of relations R that is preserved by all polynomial functions of $\mathbf{A}$ such that every function on $\mathbf{A}$ that preserves all relations in R is a polynomial function?

We develop higher commutators, which were introduced by A. Bulatov in the paper *On the number of finite Mal'tsev algebras*, Contributions to General Algebra **13**, Verlag Johannes Heyn, Klagenfurt 2001, 41–54. In our talk, we present some additional properties and alternative descriptions of higher commutators.

These properties are needed to prove that for a Mal'cev algebra $\mathbf{A}$ with congruence lattice of height two, there is a finite set of relations R that is preserved by all polynomial functions of $\mathbf{A}$ such that every function on $\mathbf{A}$ which preserves all relations in R is a polynomial function.

This is joint work with Erhard Aichinger, Institut für Algebra, Johannes Kepler Universität Linz, Austria.

Weakly representable relation algebras form a variety

Bertalan Pécsi
PhD student, ELTE University, Budapest
aladar@renyi.hu

A weakly represented relation algebra is an abstract *Boolean algebra* with extra operations (relation composition and relation inverse), the elements of which are *binary relations* on a set, the Boolean intersection is the set-theoretic one, but the Boolean complement and union are not necessarily the set-theoretic operations.

We prove that the class of algebras isomorphic to weakly represented relation algebras (wRRA's for short) is closed under taking *homomorphic images*, so it forms a variety (the cases of *subalgebras* and *products* are easy). As a consequence we classify the *subdirectly irreducible* wRRA's and prove that the congruence lattice of a wRRA is isomorphic to the congruence lattice of some Boolean Algebra.

Complex graph algebras

Agata Pilitowska
Department of Mathematics and Information Science, Warsaw University of Technology, Plac Politechniki 1, 00-661 Warsaw, Poland
apili@mini.pw.edu.pl

The complex (*power* or *global*) *algebra* $(\mathcal{P}(A), F)$ of an algebra (A, F) is the family $\mathcal{P}(A)$ of all non-empty subsets of A with complex operations given by

$$f(A_1, \ldots, A_n) := \{f(a_1, \ldots, a_n) : a_i \in A_i\},$$

where $\emptyset \neq A_1, \ldots, A_n \subseteq A$ and $f \in F$ is an n-ary operation.

Complex algebras were studied by several authors, for instance by G. Grätzer and H. Lakser [3]. They showed that for an arbitrary variety $\mathcal{V}$, the variety generated by complex algebras of algebras in $\mathcal{V}$ is determined by linear identities true in $\mathcal{V}$. They applied their result to describe all subvarieties of complex algebras of lattices and groups

In 1979 Caroline Shallon [4] introduced in her dissertation algebras associated with graphs. For an undirected graph $G = (V, E)$ with a set V of vertices and a set $E \subseteq V \times V$ of edges its *graph algebra* $A(G) = (V \cup \{0\}, \cdot)$ is a groupoid with the multiplication defined as follows:

$$x \cdot y := \begin{cases} x, & \text{if } (x, y) \in E, \\ 0, & \text{otherwise.} \end{cases}$$

From the work of C. Shallon and the characterization of finitely based graph algebras given by K. Baker, G. McNulty and H. Werner [1], it follows that a graph algebra $A(G)$ is finitely based if and only if it is entropic (a groupoid $(A, \cdot)$ is *entropic* if it satisfies the following equation: $(x \cdot y) \cdot (z \cdot w) = (x \cdot z) \cdot (y \cdot w)$).

In our talk we present the basis of all linear identities which are true in the variety of entropic graph algebras and we use it to describe the lattice of all subvarieties of complex entropic graph algebras.

Bibliography

[1] K. A. Baker, G. F. McNulty, H. Werner, The finitely based varieties of graph algebras, *Acta Scient. Math.* **51** (1987) 3–15.

[2] B. A. Davey, P. H. Idziak, W. A. Lampe, G. F. McNulty, Dualizability and graph algebras, *Discrete Math.* **214** (2000) 145–172.

[3] G. Grätzer, H. Lakser, Identities for globals (complex algebras) of algebras, *Colloq. Math.* **56** (1988) 19–29.

[4] C. R. Shallon, *Nonfinitely based binary algebras derived from lattices*, Ph.D. Thesis, University of California at Los Angeles, 1979.

Clones from ideals, part I

Michael Pinsker
Technische Universität Wien
marula@gmx.at
Coauthors: Mathias Beiglböck, Martin Goldstern, Lutz Heindorf

On an infinite base set X, every ideal of subsets of X can be associated with the clone of those operations on X which map ideal sets to ideal sets. We investigate the position of clones that arise in this way in the clone lattice. In particular we present the solution to two problems of Czédli and Heindorf and establish the existence of $2^{\mathfrak{c}}$ precomplete clones in the clone lattice over a countable set, for the first time without using the Axiom of Choice.

In part II (by M. Beiglböck), questions left open in this talk will be answered.

Remarks on the Congruence Lattice Problem

Miroslav Ploščica
Slovak Academy of Sciences, Košice
miroslav.ploscica@upjs.sk

Investigation of congruences and congruence lattices is one of the main topics in universal algebra and lattice theory. Despite intensive research, there still are many difficult and challenging problems. The Congruence Lattice Problem is the following question: *Is every distributive algebraic lattice isomorphic to the congruence lattice of a lattice?*

After more than 60 years of effort, the problem has been solved negatively by F. Wehrung in 2005. We will present the main ideas of his proof, discuss possible generalizations and open problems. Using Wehrung's technique we prove new results concerning congruence lattices of majority algebras and congruence-permutable algebras.

The free spectra of the varieties generated by idempotent semigroups

Gabriella Pluhár
ELTE, Hungary
plugab@cs.elte.hu

Let $\mathbf{A}$ be a k-element finite algebra and let $\mathcal{V}$ denote the variety generated by $\mathbf{A}$. It is known that the size of the free algebra in $\mathcal{V}$ generated by n elements ($|\mathbf{F}_{\mathcal{V}}(n)|$) is at most k^{k^n}. If $k \geq 2$, then this number is at least n. The free spectrum of a variety $\mathcal{V}$ is the sequence of cardinalities $|\mathbf{F}_{\mathcal{V}}(n)|$, $n = 0, 1, 2, \ldots$. For example, the free spectrum of Boolean algebras is $|\mathbf{F}_{\mathcal{V}}(n)| = 2^{2^n}$.

In the talk, we investigate the free spectra of varieties of idempotent semigroups, the so-called bands. We show that the free spectra of the varieties of all bands is asymptotically $\frac{1}{n^2}C^{2^n}$ for a constant C. Moreover, we show that the logarithm of the size of a free algebra in a proper subvariety of the variety of bands is $\dfrac{4}{(k-3)!}n^{k-3}\log n - \dfrac{4}{(k-3)!}n^{k-3}\sum_{j=1}^{k-3}\dfrac{1}{j} + O(n^{k-4}\log n)$, where k is an invariant of the variety.

On retract lattices of monounary algebras

Jozef Pócs
Mathematical Institute, Slovak Academy of Sciences, Košice
pocs@saske.sk
Coauthors: Danica Jakubíková-Studenovská, Faculty of Science, P.J. Šafárik University, Košice

By a retract we understand any image of an idempotent endomorphism. The system of all retracts of a given monounary algebra forms an upper semilattice. If this system contains the least element then it forms a complete lattice. We investigate the system of all retracts endowed by the empty set and also we investigate monounary algebras with the least retract. We show that the lattice of retracts of a monounary algebra is semimodular and we give a description of all monounary algebras with a complemented lattice of retracts. In particular, the lattice of retracts of a monounary algebra is complemented if and only if it is boolean. Further, we deal with the existence of a diamond in the retract lattice of a monounary algebra.

Can subalgebras determine the clone of term operations?

Reinhard Pöschel
Technische Universität Dresden
reinhard.poeschel@tu-dresden.de

Assume that for an algebra A the subalgebra lattice of A^m is known for a particular m, or for all finite powers. Under which condition this knowledge is sufficient to determine uniquely the clone of term operation of A? This and similar questions are discussed in the talk, also under the point of view of the Galois connection Pol-Inv (beween sets of functions and relations). Known results (e.g., Kearnes/Szendrei for groups or for algebras with a k-edge term operation) are reported and some new results are given for algebras A with a single n-ary operation (generalizing abelian groups or semilattices).

Length of chains in algebraic lattices

Maurice Pouzet
ICJ Mathematics Université Claude Bernard Lyon 1, Lyon, France
pouzet@univ-lyon1.fr
Coauthors: Ilham Chakir, Mathematiques, Université de Settat, Maroc

The theme of the talk is the relationship between the order structure of an algebraic lattice L and the order structure of the join-semilattice $K(L)$, made of the compact elements of L. I will concentrate on the following question: given a countable chain α, is there a finite set $\mathcal{B}$ of join semilattices such that an algebraic lattice L contains no chain of type $I(\alpha)$ (the set of initial segments of

α if and only if $K(L)$ contains no join-subsemilattice isomorphic to a member of $\mathcal{B}$.

I will present some results obtained with I. Chakir. For example, I will show that L is well-founded if and only if $K(L)$ is well-founded and does not embed, as join subsemilattices, two particular lattices. I will indicate that the question stated above, once restricted to modular algebraic lattices has a positive answer for indivisible countable chains (a typical example, after the chains ω and ω^*, is the chain of rational numbers).

Classification systems, extent partitions and context extensions

Sándor Radeleczki
Analysis Department, University of Miskolc, Hungary
`matradi@uni-miskolc.hu`
Coauthors: Bernhard Ganter, Institute of Algebra, TU Dresden, Germany, and Attila Körei, Institute of Informatical Science, University of Miskolc, Hungary

It is known that the extent partitions of a row-reduced context $K = (G, M, I)$ can be obtained by determining the classification systems of a complete atomistic lattice, which is called the box lattice of the concept lattice $B(G, M, I)$. An elementary extension K' of K is obtained by adding to the object set G a new element characterized by some attributes taken also from M. We construct the box elements of such an elementary extension and examine those extent partitions of the context K which can be extended into extent partitions of the context K'.

On representation of lattices by congruence lattices of semigroups

Vladimir Repnitskii
Ural State University
`vladimir.repnitskii@usu.ru`

A semigroup is called combinatorial if it contains no nontrivial subgroups. We obtained the following results.

Theorem 1. *Let P be a complete lattice satisfying the infinite distributive law $x \vee (\bigwedge_{i\in I}\ x_i) = \bigwedge_{i\in I}\ (x \vee x_i)$. Then the ideal lattice $I(P)$ of P is isomorphic to the congruence lattice of a combinatorial semigroup.*

Corollary. *Every finite distributive lattice is isomorphic to the congruence lattice of some combinatorial semigroup.*

Theorem 2. *Every distributive algebraic lattice with at most countably many compact elements is isomorphic to the congruence lattice of a [countable] combinatorial semigroup.*

The existence of states on effect algebras

Zdenka Riečanová
Department of mathematics, FEI STU
zdenka.riecanova@stuba.sk
Coauthors: Wu Junde, Katarina Mosna

The existence of states on effect algebras (even orthomodular lattices) is still an open question. Nevertheless we can obtain positive results for some families of lattice ordered effect algebras. Namely we can obtain statements about the existence of two-valued states on atomic lattice effect algebras.

Convex sets and fuzzy logics

Anna Romanowska
Warsaw University of Technology, Faculty of Math. and Info. Sci., Warsaw, Poland
aroman@mini.pw.edu.pl
Coauthors: J. D. H. Smith (Iowa State University, Ames, Iowa, USA), E. Orlowska (National Institute of Telecommunications, Warsaw, Poland)

It is well known that real convex sets can be presented as algebras with the binary basic operations $x(1-p)+yp$ of weighted means, for each p in the open unit interval of real numbers. The class of such algebras is a quasivariety and generates the variety of so-called barycentric algebras. Both these classes have a well developed theory. However one question was still open. For the definitions and axiomatizations of convex sets and barycentric algebras we had to use the open unit interval, that was not axiomatized in abstract way till recently. This talk will discuss the problem of axiomatization and will show one possible solution. The class of traditional barycentric algebras will be extended to a class of two-sorted algebras, where one of the sorts corresponds to a certain algebra of fuzzy logic. The new structures encompass two-sorted counterparts of all barycentric algebras over any ordered field, and contain also some other algebras providing links to such notions as Boolean affine spaces, B-sets of Bergman and Stokes, and "if-then-else" algebras.

On the Hilbert ideals of a cyclic group of prime order

Müfit Sezer
Boğaziçi University, Istanbul, Turkey
mufit.sezer@boun.edu.tr

The Hilbert ideal is the ideal generated by positive degree invariant polynomials of a finite group. For a cyclic group of prime order p, we show that invariant polynomials that are the fixed points of free modules are in the ideal generated by invariants of degree at most $p-1$. Consequently we show that the Hilbert ideal corresponding to an indecomposable representation is generated by polynomials of degree at most p, confirming a conjecture of Harm Derksen and Gregor Kemper for this case.

From quantale algebras to topological spaces

Sergejs Solovjovs
Department of Mathematics, University of Latvia
sergejs@lu.lv

The notion of fuzzy set introduced by Zadeh induced many lines of research to study different fuzzy structures. In particular, numerous papers consider fixed-basis as well as variable-basis fuzzy topologies and its properties. Following the general move we considered a relation between the categories Q-**Alg** of Q-algebras and Q-**Top** of weakly stratified Q-topological spaces for a given unital commutative quantale Q. We tried to generalize the following well-known result: "Let **Top** be the category of topological spaces and let **Loc** be the category of locales. The functor **Top** $\to$ **Loc** which sends a space X to its lattice of open sets $O(X)$ and a continuous map $f : X \to Y$ to the function $f^{\leftarrow} : O(Y) \to O(X)$ has a right adjoint." By the aforesaid result it follows that the category **Loc** is an appropriate environment in which to develop topology. It appears that there exists quite as good a relation between the categories (Q-**Alg**)^{op} and Q-**Top**. In particular, one has a pair of adjoint functors between them. Moreover, appropriate changes in the definitions of sobriety and spatiality give an equivalence between the categories of Q-sober Q-topological spaces and Q-spatial Q-algebras. As a result of all these investigations one gets a good substitute for the category **Loc** in case of fixed-basis fuzzy topologies, i.e., an environment for developing point-free fixed-basis fuzzy topologies. It is the purpose of this talk to present the obtained results.

Subreducts of modules over commutative rings
Michał Stronkowski
Warsaw University of Technology, Faculty of Math. and Info. Sci., Warsaw, Poland
m.stronkowski@mini.pw.edu.pl

A mode is an entropic and idempotent algebra. Romanowska-Smith theorem states that each cancellative mode is a subreduct of a module over a commutative ring. We are interested in investigating to what extent the assumptions of this theorem may be weakened. In this talk it will be shown that idempotency is in fact irrelevant.

Subrings which are closed with respect to taking the inverse
Jenő Szigeti
University of Miskolc, Hungary
jeno.szigeti@uni-miskolc.hu
Coauthors: Leon van Wyk

Let S be a subring of the ring R. We investigate the question of whether

$$S \cap U(R) = U(S)$$

holds for the units. In many situations our answer is positive. There is a special emphasis on the case when R is a full matrix ring and S is a structural subring of R defined by a reflexive and transitive relation.

A property af CP varieties having SDPC
Boža Tasić
Ryerson University, Toronto, Canada
btasic@ryerson.ca

The variety $\mathbf{R}_c$ of commutative rings with identity is congruence permutable (CP) and has definable principal congruences by a special first order formula (SDPC). The varieties having CP and SDPC satisfy some special inequalities among the operators H, S and P_f (H for homomorphic images, S for subalgebras, P_f for filtered products). We will give some of the inequalities and as a corollary we will describe the standard monoid of the variety $\mathbf{R}_c$ generated by the operators H, S, P_f.

Axiomatic extensions of monoidal logic

Esko Turunen
Tampere University of Technology
esko.turunen@tut.fi
Coauthors: Janne Mertanen

Ulrich Höhle introduced Monoidal Logic in 1995 in order to give a common framework to several first order non-classical logics, such as Linear logic, Intuitionistic logic and Lukasiewicz logic. The main tool to prove the completeness of these logics was to construct a canonical model by means of MacNeille completion. In this work we present new axiomatic extensions of Monoidal logic, namely Semi-divisible logic, weak MTL and weak BL logic. We prove that these non-classical logics are complete with respect to the corresponding complete algebraic structures in the same sense that Classical predicate logic is complete with respect to complete Boolean algebras.

Semidirect sum of semilattices revisited

Edouard Wagneur
École Polytechnique de Montréal & GERAD, Montréal, Canada
Edouard.Wagneur@gerad.ca
Coauthors: Farba Faye, Université Cheikh Anta Diop de Dakar, Senegal

In classical module theory, a module over a principal ideal domain may be decomposed into a direct sum of a free module, and a torsion module. This decomposition is induced by the decomposition of the abelian group structure of modules, and allows for the classification of modules over principal ideal domains.

In the context of idempotent semimodules the concept of semi-direct sum – a generalization of direct sum – has been defined in [1]. Since a semimodule over a semiring is a commutative monoid, such an extension to idempotent semimodules need also be defined for idempotent commutative monoids, i.e., to semilattices. The aim of this paper is to show how the semi-direct sum decomposition of a semilattice S into $S_1 \tilde{\oplus} S_2$ of [1] can be expressed as a quotient of the cartesian product $S_1 \times S_2$.

References

[1] E. Wagneur, Dequantization: Semi-direct Sums of Idempotent Semimodules, *Contemporary Mathematics,* **377**, 339–352, 2005.

Research supported by NRC grant RGPIN-143068-05

Almost associative operations generating a minimal clone

Tamás Waldhauser
University of Szeged, Hungary
twaldha@math.u-szeged.hu

The characterization of minimal clones in full generality is a very hard (perhaps impossible) problem; all known results describe minimal clones under some restrictions. One possibility is to determine minimal clones generated by an operation satisfying certain identities. Probably the most natural question of this kind is to characterize semigroups with a minimal clone. This problem has been solved by M. B. Szendrei almost 30 years ago. The aim of this talk is to present some generalizations of this result. There are several ways to measure how far a given binary operation is from being associative. Each such 'associativity measure' gives rise to a notion of 'almost associativity'. We describe minimal clones generated by almost associative operations for two different interpretations of almost associativity.

Implicational concept graphs

Rudolf Wille
TU Darmstadt, Mathematics Department, D-64289 Darmstadt
wille@mathematik.tu-darmstadt.de

Implicational concept graphs give rise to a mathematical semantics of implications. The advantage of the mathematical semantics offered is that it opens the door to mathematical structure theory with its rich structural insights and patterns of argumentations. As a consequence, it could be proved that the implicational theory of implicational concept graphs is equivalent (in the main) to the theory of attribute implications of formal contexts. This result could even be generalized to an analogue result for clausal concept graphs.

Categories of motives for additive categories

Anatoly Yakovlev
St. Petersburg State University
yakovlev.anatoly@gmail.com

Let $\mathfrak{A}$ be an additive category; for any associative ring Λ with 1 denote by $M_\Lambda(\mathfrak{A})$ the category, the objects of which are pairs (A, e), where A is an object of the category and e an idempotent element of the ring $\Lambda \otimes \mathrm{End}_{\mathfrak{A}}(A)$, and the groups of homomorphisms are defined as follows:

$$\mathrm{Hom}_{M_\Lambda(\mathfrak{A})}((A,e),(B,d)) = d(\Lambda \otimes \mathrm{Hom}_{\mathfrak{A}}(A,B))e \subseteq \Lambda \otimes \mathrm{Hom}_{\mathfrak{A}}(A,B).$$

It is natural to call the category $M_\Lambda(\mathfrak{A})$ *the category of* Λ*-motives*, and the category $M_{\mathbb{Z}}(\mathfrak{A})$ *the category of motives* for the category $\mathfrak{A}$.

Fix the category $\mathfrak{A}$ and introduce notation:

$$M = M_{\mathbb{Z}}(\mathfrak{A}), \quad M_p = M_{\mathbb{Z}_p}(\mathfrak{A}), \quad M_0 = M_{\mathbb{Q}}(\mathfrak{A}), \quad M_\infty = M_{\mathbb{C}}(\mathfrak{A}),$$

where, as usual, $\mathbb{Z}, \mathbb{Z}_p, \mathbb{Q}, \mathbb{C}$ stay for the rings of integers and p-adic integers and the fields of rational and complex numbers. For every p fix an embedding of the ring $\mathbb{Z}_p$ in $\mathbb{C}$; together with the natural embeddings $\mathbb{Z} \to \mathbb{Q}, \mathbb{Z}_p, \quad \mathbb{Q} \to \mathbb{C}$ they induce functors which constitute the following commutative diagram:

$$\begin{array}{ccc} M & \xrightarrow{F_0} & M_0 \\ {\scriptstyle F_p}\big\downarrow & & \big\downarrow{\scriptstyle G_0} \\ M_p & \xrightarrow[G_p]{} & M_\infty \end{array}$$

It is easy to prove that the functor G_p does not depend on the choice of the embedding $\mathbb{Z}_p \hookrightarrow \mathbb{C}$.

Theorem *Let $\mathfrak{A}$ be an additive category such that the additive group of the endomorphism ring $E = E_A$ of any object A of $\mathfrak{A}$ has the property: let $T(E)$ be the group of all periodic elements of E; then $E/T(E)$ is a group of finite rank, and all p-components of $T(E)$ are finite.*

1. *The Krull-Schmidt theorem holds in the categories M_0, M_p, M_∞ (but not in M !)*

2. *If A, B are objects of the category M, such that $F_p(A)$ and $F_p(B)$ are isomorphic objects of the category M_p for $p = 0$ and for all prime integers p, and if $A = X \oplus Y$, then there is a decomposition $B = X' \oplus Y'$ such that $F_p(X) \approx F_p(X')$, $F_p(Y) \approx F_p(Y')$ for $p = 0$ and for all prime integers p.*

3. *For every prime integer p and for $p = 0$ chose an object X_p of the category M_p. If for every prime integer p the objects $G_p(X_p)$ and $G_0(X_0)$ of the category M_∞ are isomorphic, and almost all objects X_p are trivial in a certain sense (which we do not specify here), then there exists an object A of the category M such that $F_0(A) \approx X_0$ and $F_p(A) \approx X_p$ for all prime integers p.*

Solvability of systems of polynomial equations over finite algebras

László Zádori
University of Szeged
`zadori@math.u-szeged.hu`

The talk is on the algorithmic complexity of determining whether a system of polynomial equations over a finite algebra admits a solution. I have recently proved that the problem has a dichotomy in the class of finite groupoids with

an identity element. By developing the underlying idea further I present a dichotomy theorem in the class of finite algebras that admit a nontrivial idempotent Maltsev condition. This is a substantial extension of most of the earlier results on the topic.