Вторая конференция Математических центров России
Секция «Математическая логика и теоретическая информатика»

7–11 ноября 2022, Москва

Н. А. Баженов. On spectrally universal classes of structures

For a countable algebraic structure S, the degree spectrum of S is the set of Turing degrees of all isomorphic copies of S. A class of structures K is *spectrally universal* if for every countable structure S, there exists a structure M from K such that the degree spectra of M and S are the same. The talk discusses recent results on spectral universality for some familiar algebraic classes: modal algebras, contact Boolean algebras, Heyting algebras with distinguished atoms and coatoms.

The work is supported by the Mathematical Center in Akademgorodok under the agreement No. 075-15-2022-281 with the Ministry of Science and Higher Education of the Russian Federation.

И. И. Батыршин. Счетная строгая обратная математика

Строгая обратная математика — это предложенная Х. Фридманом программа исследований, целью которой является изучение логической силы математических теорем с помощью строго математических аксиом и без использования кодирования. В качестве базовой теории для счетной строгой обратной математики Фридманом была предложена элементарная теория функций ETF. В докладе предполагается обсудить подсистемы ETF и их эквивалентные аксиоматизации. Краткая аннотация доклада.

Б. Ф. Л. Баувенс. Fast dynamic matching in bipartite lossless expanders

We consider bipartite graphs, and refer to the 2 parts as left and right nodes. Hall's theorem states that if every set S of left nodes has at least $\#S$ neighbors, then the graph has a matching that saturates all the left nodes. We say that a graph has e-expansion up to K elements, then if every left set S of size at most K has at least $e\#S$ neighbors. Thus Hall's theorem implies that if a graph has 1-expansion up to K, then every left set of size K has a saturating matching. We consider a dynamic variant of this problem and present a strategy that can be solved in time O(D polylog N) in graphs with N left nodes and left degree at most D. However, the algorithm only works in graphs with (2D/3)-expansion. Such graphs can be computed using with known constructions.

Application 1: 1-bit probes. Such probes are datastructures to store a set S and in which a membership query is answered probabilistically by reading only a single bit from the memory. Our construction reduces the size of the smallest such probes. Moreover, our probes are dynamic: one can add and remove elements in S.

Application 2: connector graphs. Such graphs model the connection problem on old telephone networks in which input and output nodes need to be connected using node disjoint paths. Our algorithm gives an almost double exponential speed up of the path finding algorithm in constant depth connectors, and this solves an open question by Feldman, Friedman and Pippenger from 1988.

М. В. Волков. Synchronizing quantum automata

In the literature, there exists many definitions of quantum automata (QA). Their common feature is that the role of a state set is played by a finite-dimensional Hilbert space H while the role of a finite input alphabet is played by a bunch Σ of linear transformations of H. QA are mostly studied from the viewpoint of language recognition.

In the talk, I treat QA as protocols rather than recognizers and suggest the notion of synchronizing QA. The model of QA I consider is similar to the well-known measure-once model by Moore and Crutchfield with the only difference that the measurement is partial and the computation continues after the measurement. Such an automaton is said to be synchronizing if there is a word w over Σ such that the result of the consecutive application of transformations forming w does not depend on the outcome of the measurement step.

I will present a few examples and discuss open questions.

С. С. Гончаров. Логический подход к проблемам управления и ИИ в рамках семантического моделирования

В докладе будут изложены идеи и результаты предложенного Ю. Л. Ершовым, С. С. Гончаровым и Д. И. Свириденко логического подхода в рамках семантического моделирования для построения математических методов доверительного ИИ и построения управления сложными объектами на основе теоретико-модельных конструкций построения наследственно конечных списочных расширений абстрактных моделей и логического языка для определения вычислимости над абстрактными моделями. Исходные идеи для данного подхода базируются как на теории вычислимости и теории моделей, так и на развитии идей теории допустимых множеств. Исследования посвящены алгоритмическим свойствам языка и его семантики, включая проблемы полиномиальности строящихся алгоритмов как над языковыми конструкциями, так и над моделями, а также теоретико-модельным свойствам и связям различных конструкций. Важным элементом данных исследований являются и методы реализации в практических реализациях и возникающих при этом новых проблемах и задачах.

С. М. Дудаков. On properties of subsets algebras

Any operation over any domain can be generalized on arbitrary subsets of the domain. So for any universe we can consider algebras of subsets with the same operations. It can be algebra of all subsets or some subsets, for example, finite subsets. We investigate subsets algebras for various original universes. We have established results on elementary equivalence, algorithmic decidability, definability, and other properties.

We pay special attention to semigroups. The free semigroup is the algebra of all words with concatenation. So the subsets algebras is the corresponding algebras of languages. Another examples are subsets of natural numbers or unity-coefficient polynomials over any idempotent semiring with unity.

Another universes we consider are unars with an injective function. Then the subsets algebras are of the same kind. We have established structure of its theory.

А. А. Запрягаев. Interpretations of Büchi arithmetics in themselves

Büchi arithmetics BA_n, $n \geqslant 2$, are extensions of Presburger arithmetic with an unary functional symbol $V_n(x)$ denoting the largest power of n that divides x. These theories were introduced by J. Büchi in order to describe the recognizability of sets of natural numbers by finite automata through definability in some arithmetical language. As shown by V. Bruyère, the definability of a set of natural numbers in BA_n is equivalent to its recognizability by a finite automaton receiving m-tuples of natural numbers in the form of m-tuples of their last, then penultimate, etc. digits of their n-ary expansion.

A. Visser has asked the following question: given an weak arithmetical theory T without ability to encode syntax but with full induction, does it hold that each interpretation (one-dimensional or multi-dimensional) of T into itself is isomorphic to the trivial one, and, if it is, is the isomorphism always expressible by a formula of T? This question was previously answered positively for Presburger arithmetic PrA in the author's joint work with F. Pakhomov.

We show that each interpretation of BA_n itself in its own standard model N and show that each such interpretation is isomorphic to the trivial one. Furthermore, we obtain this result already for the interpretations of Presburger Arithmetic in BA_n. The proof is based on the contradiction between a condition on automatic torsion-free abelian groups given by Braun and Strüngmann and the description of the order types of non-standard models of Büchi arithmetics. This gives a partial positive answer to the question of Visser.

М. В. Зубков. Well-orders realized by CE equivalence relations

A structure A is realized by an equivalence relation E if there exists a structure B such that B/E is isomorphic to A. We will describe sets of ordinals that can be realized by one fixed computably enumerable equivalence relation, provided that this equivalence relation can realize an ordinal less than ω^ω.

(Joint work with N. A. Bazhenov.)

В. Г. Кановей. О существенности параметров в схеме аксиом свертки в арифметике второго порядка

Построена модель арифметики второго порядка, в которой аксиома свертки верна в беспараметрическом варианте но не верна в полном варианте с параметрами.

К. А. Ковалев. Analogues of Shepherdson's Theorem for the arithmetical language with exponentiation

We investigate the following expansions of IOpen (Robinson arithmetic Q with quantifier-free induction):

- IOpen(exp): Q with axioms $\exp(0) = 1$ and $\exp(Sx) = exp(x) + exp(x)$ and quantifier-free induction in the expanded language;
- IOpen(x^y): Q with axioms $x^0 = 1$ and $x^{(}Sy) = (x^y) \cdot x$ and quantifier-free induction in the expanded language.

In 1964 Shepherdson proved the following theorem characterizing models of IOpen: For every discretely ordered ring M, the nonnegative part M^+ is a model of IOpen iff M is an integer part

of the real closure $R(M)$ of the fraction field of M (i.e. for every $r \in R(M)$ exists $m \in M$ such that $m \leqslant r < m + 1$).

Our purpose is to generalize this theorem to the expanded theories IOpen(exp) and IOpen(x^y). We obtain some partial results for these theories and a full analogue of the Shepherdson's theorem for the theory IOpen + T_{x^y}, where the latter is some finite set of the natural properties of exponentiation.

М. В. Коровина. Automated reasoning with continuous data

In this talk we report on ongoing research on solving non-linear constraints over the reals occurring in a wide range of applications, starting with program verification, ranging over verification of real-world designs all the way to automation of formally verified proofs of mathematical statements.

In our framework methods from Computable Analysis and Automated Reasoning are combined to meet efficiency and expressiveness. This approach is applicable to a large number of constraints involving computable non-linear functions, piecewise polynomial splines, transcendental functions and solutions of polynomial differential equations.

We give an introduction to the ksmt calculus for checking satisfiability of non-linear constraints in a CDCL style way inspired by advances in SAT solving. Along proof search ksmt resolves two types of conflicts: linear and non-linear. Linear conflicts are delegated to a decision procedure for linear real arithmetic and non-linear conflicts are resolved by local linearisations separating the solution set and the current conflict. We show that the ksmt calculus is a δ-complete decision procedure for bounded problems.

И. А. Михайлин. Полиномиальные формулировки как барьер для доказательств сложности

Теория сложности пытается ответить на вопросы о минимальном количестве ресурсов необходимых на решение алгоритмической задачи. В классическом варианте ответ на такой вопрос представляется в виде отнесение задачи к какому-то сложностному классу, например к классу P — задачам решаемым за полиномиальное время. При этом решается задача за n^2 или за n^{100} уже неважно. В последние годы активно развивается другой подход известный как теория высокоточных оценок, где сложность решение задач пытаются измерить наоборот максимально точно. Поскольку у нас пока нет примеров безусловных оценок на сложность задач, эта теория оперерует нижними оценками в предположении различных гипотез. В этом докладе мы поговорим о том как такие оценки доказываются в предположении Strong exponential time hypothesis и почему для каких-то задач такие нижние оценки будут иметь невероятно сильные последствия для других областей теории сложности. Доклад будет состоять из обзорной части и краткого разговора о нашей последней статье “Polynomial formulations as a barrier for reduction-based hardness proofs”.

А. А. Оноприенко. On topological models of intuitionistic epistemic logic

The intuitionistic logic H4 with the modality of knowledge is in some way dual to the classical modal logic S4. I will talk about two types of topological models of the logic H4: models with a dense distinguished subset, as well as bitopological models.

В. Н. Ореховский. О логических и топологических классификациях регулярных омега-языков

В работе рассматриваются два подхода к классификации ω-языков: логический и топологический. При первом подходе ω-слова рассматриваются как структуры сигнатуры $\sigma = \{\leqslant, Q_a, ...\}$ или $\tau = \sigma \cup \{p, s\}$. Получим иерархии Σ_n^σ и Σ_n^τ, индуцируемые иерархиями предложений сигнатур σ и τ по числу перемен кванторов в предваренной нормальной форме. При втором подходе на множестве A^ω вводится канторовская топология и рассматривается борелевская иерархия $\mathbf{\Sigma}_n^0$. Также рассматриваются тонкие иерархии (Selivanov 1998) $\mathcal{S}_\alpha$ и $\mathbf{\Sigma}_\alpha$. Последняя на множестве регулярных ω-языков совпадает с иерархией Вагнера (Wagner 1979). Известно, что $\bigcup_{\alpha<\omega^\omega} \mathcal{S}_\alpha = BC(\Sigma_2^\sigma)$ и $\bigcup_{\alpha<\omega^\omega} \mathbf{\Sigma}_\alpha = BC(\mathbf{\Sigma}_2^0)$.

Основным результатом данной работы является полное описание соответствия между логическими и топологическими классификациями.

Т. Г. Пшеницын. Commutative Lambek grammars are not context-free

In 1993, Mati Pentus proved that Lambek grammars are equivalent to context-free grammars in the sense that they generate the same set of languages (disregarding the empty word). We prove that a similar result does not hold for grammars over the Lambek calculus with permutation (LP), which can also be called commutative Lambek grammars. More precisely, we show that there is a language that can be generated by a commutative Lambek grammar such that it is not a permutation closure of a context-free language. To prove this, we present a formalism equivalent to commutative Lambek grammars, which we call linearly-restricted branching vector addition systems with states; it is simpler to establish the desired result for them.

В. В. Рыбаков. Temporal multi-agent logics, problems satisfiability, decidability and admissibility

In our research we investigate temporal multi-agent logics with various possible non-transitive temporal accessibility relations. Main idea of this choice consists in attempts more precisely model and describe behavior, reasoning and computation agents (distinct acting computational threads) when they cooperate and acts mutually. In particular, we consider non-transitive logics, where elements of interval logics are applied. In this case the time accessibility relations are non-transitive and chopped into intervals of bounded time. In definition of models, we consider logics with only one objective valuation of propositional states and logics with multi-valuations — the case when the agents have separated own valuations' relations for propositions.

Looking at the case when the time accessibility relations may be affected by events and alter during computation we study logics which have dynamic accessibility relations — the case when any state (world) generates (and hence have) its own accessibility relation. Mathematical problems we are dealing with are problems of satisfiability, decidability and admissibility. Found computational algorithms to be reported.

Supported by the Krasnoyarsk Mathematical Center and financed by the Ministry of Science and Higher Education of the Russian Federation (Grant No. 075-02-2020-1534/1) and by Research Program at the National Research University Higher School of Economics (HSE University) Moscow.

М. Н. Рыбаков. Undecidability of modal and superintuitionistic logics of a single unary predicate in languages with two variables

We consider the issues concerning algorithmic complexity of non-classical predicate logics in restricted languages. In 1962, S. Kripke suggested how to simulate a binary predicate letter of a classical first-order formula with a modal first-order formula containing two unary letters. Building on Kripke's idea, we simulate a binary precidate letter with a single unary letter in modal formulas and with two unary letters in superintuitionistic formulas. This immediately gives us the undecidability of numerous modal logics in languages with one unary letter, and superintuitionistic logics with two unary letters, and three variables, since the classical logic of a binary predicate is undecidable with three variables. In addition, we show how to simulate any number of unary letters with a single unary letter (both in modal and intuitionistic languages). Due to the well-known results on the undecidability of many non-classical logics in languages with two variables (D. Gabbay, V. Shehtman (1993), R. Konchakov, A. Kurucz, M. Zakharyaschev (2005)), we obtain the undecidability of many modal and superintuitionistic predicate logics in languages with a single unary predicate letter and two variables. The proposed encoding enables us to obtain the non-enumerability and even non-arithmeticity of the corresponding fragments of a number of logics of Kripke frames. Our results extend to polymodal logics, such as predicate counterparts of CTL*, CTL, LTL, epistemic logics, logics with universal modality, etc.

В. Л. Селиванов. Boole vs Wadge: comparing basic tools of descriptive set theory

We systematically compare omega-Boolean classes (obtained from open sets (or other classes) by applying omega-Boolean operations), the reducibility by continuous functions (known as Wadge reducibility), and the recent extension of Wadge hierarchy to non-zero-dimensional spaces. E.g., we complement the result of W. Wadge that the collection of non-self-dual levels of his hierarchy coincides with the collection of classes generated by Borel omega-ary Boolean operations from the open sets in the Baire space. Namely, we characterize the operations, which generate any given level in this way, in terms of the Wadge hierarchy in the Scott domain. As a corollary we deduce the non-collapse of the latter hierarchy. Also, the effective version of this topic is discussed.

А. А. Семенов, С. Е. Кочемазов. Using Backdoors to estimate the hardness of Boolean formulas w.r.t. SAT solving algorithms

The Boolean satisfiability problem (SAT) is a classical combinatorial problem which is NP-complete in the decision variant and NP-hard in the search variant. Nevertheless, during the recent 20 years there have been developed a lot of applied algorithms that successfully tackle SAT for formulas of large dimension (tens of thousands of variables and hundreds of thousands of clauses). These algorithms called SAT solvers are routinely used in such areas as symbolic verification, program testing, cryptanalysis, bioinformatics, combinatorics, etc. Despite the impressive effectiveness of modern SAT solvers, it is often important to know in advance their approximate runtime on particular formulas. It is a typical situation that a SAT solver has been working for an hour or a day or a month, and it is not known whether it will finish anytime soon. The question then is whether it is possible to construct some meaningful upper bounds on the runtime of a particular SAT solver on a particular SAT instance? In the report we will present several results in this direction. The presented approach is based on the idea to evaluate the hardness of a formula via some decomposition or, in a more general case, via a so-called SAT

partitioning of a formula. In order to construct such a partitioning we choose a set called Backdoor and decompose an original formula into sub-formulas by substituting all possible combinations of values of backdoor variables to a formula. Then, under certain assumptions we can use the Monte Carlo method to estimate the runtime of a solver on the original formula via its runtimes on formulas from a constructed decomposition. On the level of ideas, the proposed estimations are quite close to the hardness estimations that are constructed based on the knowledge of the so-called Strong Backdoor Sets. In the report we will show the interconnection between Strong Backdoors and the proposed notions, and present the results of computational experiments which demonstrate the practical applicability using backdoors to estimate the hardness of Boolean formulas. We will also briefly describe the basic algorithms and techniques used in state-of-the-art SAT solvers.

А. Л. Семёнов, С. Ф. Сопрунов. Recent results on definability lattices of numerical structures

Definability is one of the central concepts of mathematical logic and is one of the important concepts of all mathematics. At the same time, it is still relatively little studied.

The report will discuss the latest results related to definability lattices (reduct lattices) for numerical structures, such as, for example, the addition of rational numbers.

It is remarkable that a number of these results were obtained by high-school students at the May 2022 Program in "Sirius".

М. Х. Файзрахманов. Generalized computable numberings and fixed points

The talk considers generalized computable numberings from the point of view of uniform enumerability of numbered families relative to arbitrary oracles. The results presented are aimed at classifying oracles such that all (principal) families computable in them have generalized computable numberings that satisfy the Kleene fixed point theorem with different degrees of uniformity: complete and precomplete numberings, weakly precomplete numberings, and also numberings that satisfy the Recursion theorem and the Recursion theorem with parameters.

C. Хетцль. Logical analysis of automated inductive theorem proving

Automating the search for proofs by induction is an imporant topic in computer science with a history that stretches back decades. A variety of different approaches and systems has been developed. Typically, these systems have been evaluated empirically and thus very little is known about their theoretical limitations.

In this talk I will show how to use mathematical logic to understand the theoretical power and limits of methods for automated inductive theorem proving. A central tool are translations of proof systems that are intended for automated proof search into (very) weak arithmetical theories. Thus unprovability results can be transferred from theories to methods of automated deduction.

I will describe concrete such analyses of two methods of automated inductive theorem proving including practically relevant unprovability results: 1. adding explicit induction axioms to a saturation theorem prover and 2. clause set cycles.

(Joint work with Jannik Vierling.)

М. В. Швидефски. Dualities for categories of partially ordered structures

We present recent categorical duality results for certain categories of partially ordered sets (lattices) and certain categories of topological spaces endowed with some additional structure. Some

of these results extend classical duality results by M.H. Stone. (Supported by the Mathematical Center in Akademgorodok, agreement with Ministry of Science and Higher Education of Russia № 075-15-2022-282.)

В. Б. Шехтман. How to axiomatize boxing of a modal predicate logic?

Boxing of a modal predicate logic L is defined as the minimal logic containing all formulas $\Box A$, where A is a theorem of L. For axiomatization of boxing it is usually insufficient just to add $\Box$ to axioms of L. The general problem of axiomatization of boxing was put in our talk "Boxing modal logics" at Logical Perspectives 2021. This problem is solved in the paper "On Kripke completeness of modal predicate logics around quantifed K5" (forthcoming in APAL).

The recipe is the following: take all possible shifts of the axioms, then take their universal closures with $\Box$ added. An n-shift of a predicate formula A is obtained by increasing arities of all predicate letters by n and adding fixed n new parameters to all atoms occurring in A. In general this yields infinitely many axioms, but in many cases (described in the same talk and paper) 1-shifts are sufficient, so boxing preserves finite axiomatizability.

Our conjecture is that boxing of the finitely axiomatizable logic QKAlt_1 (where Alt_1 is the axiom of unique successor) is not finitely axiomatizable. The proof of this conjecture probably requires a nontrivial model-theoretic technique. In the talk we describe the first step on the way to the proof: 1-shifts are insufficient in this case.